ID: 878476
Sample Name: main2.dll
Cookbook: default.jbs
Time: 18:08:34
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

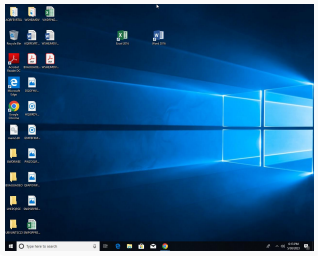
Windows Analysis Report

main2.dll

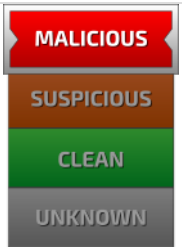
Overview

General Information

Sample Name:	main2.dll
Analysis ID:	878476
MD5:	5e107608dd00…
SHA1:	d9bfa3e88ca0f…
SHA256:	185737016a01…
Tags:	dll
Infos:	



Detection



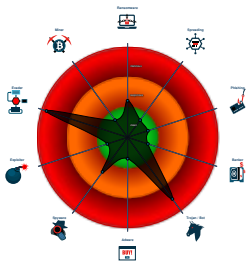
Qbot

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: 7380 cmdline: loaddll32.exe "C:\Users\user\Desktop\main2.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 7388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7416 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\main2.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7436 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 7528 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7436 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7424 cmdline: rundll32.exe C:\Users\user\Desktop\main2.dll,mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7536 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7424 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7644 cmdline: rundll32.exe C:\Users\user\Desktop\main2.dll,mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7672 cmdline: rundll32.exe C:\Users\user\Desktop\main2.dll,mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7708 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7672 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7768 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7916 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7768 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7796 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7808 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7932 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7808 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7816 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 8032 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
      - ipconfig.exe (PID: 7132 cmdline: ipconfig /all MD5: B0C7423D02A007461C850CD0DFE09318)
        - conhost.exe (PID: 7136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 3124 cmdline: whoami /all MD5: 2E498B32E15CD7C0177A254E2410559C)
        - conhost.exe (PID: 7880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 7836 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",mvutil_license MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7844 cmdline: rundll32.exe "C:\Users\user\Desktop\main2.dll",mvutil_configuration MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- msiexec.exe (PID: 3780 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": "obama265",
  "Campaign": "1685436052",
  "Version": "404.1320",
  "C2 list": [
    "103.42.86.42:995",
    "174.4.89.3:443",
    "161.142.103.187:995",
    "78.160.146.127:443",
    "84.35.26.14:995",
    "12.172.173.82:20",
    "70.28.50.223:2078",
    "124.149.143.189:2222",
    "70.160.67.203:443",
    "186.64.67.30:443",
    "103.123.223.133:443",
    "94.207.104.225:443",
    "89.114.140.100:443",
    "213.64.33.61:2222",
    "86.176.144.234:2222",
    "72.134.124.16:443",
    "47.34.30.133:443",
    "109.50.149.241:2222",
    "85.104.105.67:443",
    "81.111.108.123:443",
    "86.173.2.12:2222",
    "188.28.19.84:443",
    "41.228.224.161:995",
    "12.172.173.82:50001",
    "178.175.187.254:443",
    "65.95.141.84:2222",
    "205.237.67.69:995",
    "83.110.223.61:443",
    "193.253.100.236:2222",
    "27.0.48.233:443",
    "102.159.188.125:443",
    "71.38.155.217:443",
    "58.186.75.42:443",
    "76.178.148.107:2222",
    "70.28.50.223:2087",
    "114.143.176.236:443",
    "51.14.29.227:2222",
    "59.28.84.65:443",
    "173.88.135.179:443",
    "103.144.201.56:2078",
    "96.87.28.170:2222",
    "105.184.103.97:995",
    "176.142.207.63:443",
    "151.62.238.176:443",
    "12.172.173.82:32101",
    "122.186.210.254:443",
    "82.125.44.236:2222",
    "84.108.200.161:443",
    "76.16.49.134:443",
    "70.28.50.223:32100",
    "12.172.173.82:465",
    "76.170.252.153:995",
    "184.182.66.109:443",
    "78.92.133.215:443",
    "50.68.204.71:993",
    "186.75.95.6:443",
    "113.11.92.30:443",
    "70.28.50.223:3389",
    "98.145.23.67:443",
    "85.57.212.13:3389",
```

```
      "50.68.186.195:443",
      "47.205.25.170:443",
      "12.172.173.82:993",
      "12.172.173.82:22",
      "69.242.31.249:443",
      "81.101.185.146:443",
      "79.168.224.165:2222",
      "75.143.236.149:443",
      "14.192.241.76:995",
      "86.195.14.72:2222",
      "81.229.117.95:2222",
      "220.240.164.182:443",
      "73.29.92.128:443",
      "12.172.173.82:21",
      "96.56.197.26:2222",
      "75.109.111.89:443",
      "76.86.31.59:443",
      "201.244.108.183:995",
      "68.203.69.96:443",
      "124.122.47.148:443",
      "122.184.143.86:443",
      "92.186.69.229:2222",
      "70.28.50.223:2083",
      "89.129.109.27:2222",
      "147.147.30.126:2222",
      "125.99.76.102:443",
      "88.126.94.4:50000",
      "151.65.167.77:443",
      "86.132.236.117:443",
      "92.154.17.149:2222",
      "223.166.13.95:995",
      "89.36.206.69:995",
      "96.56.197.26:2083",
      "78.18.105.11:443",
      "82.127.153.75:2222",
      "90.78.147.141:2222",
      "82.131.141.209:443",
      "183.87.163.165:443",
      "92.9.45.20:2222",
      "80.6.50.34:443",
      "80.12.88.148:2222",
      "69.133.162.35:443",
      "172.115.17.50:443",
      "95.45.50.93:2222",
      "12.172.173.82:2087",
      "103.140.174.20:2222",
      "24.198.114.130:995",
      "50.68.204.71:443",
      "69.119.123.159:2222",
      "64.121.161.102:443",
      "2.82.8.80:443",
      "184.181.75.148:443",
      "70.112.206.5:443",
      "198.2.51.242:993",
      "2.36.64.159:2078",
      "79.77.142.22:2222",
      "84.215.202.8:443",
      "147.219.4.194:443",
      "116.74.164.81:443",
      "70.28.50.223:2078"
    ]
  }
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.407663354.00000000004FA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000011.00000002.409110977.0000000000E30000.00000004.00000020.00020000.00000000.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
17.2.rundll32.exe.511128.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xdf71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9b97:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
17.2.rundll32.exe.511128.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
17.2.rundll32.exe.7c0000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
17.2.rundll32.exe.7c0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
17.2.rundll32.exe.511128.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
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)

Anti Debugging

Potentially malicious time measurement code found

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

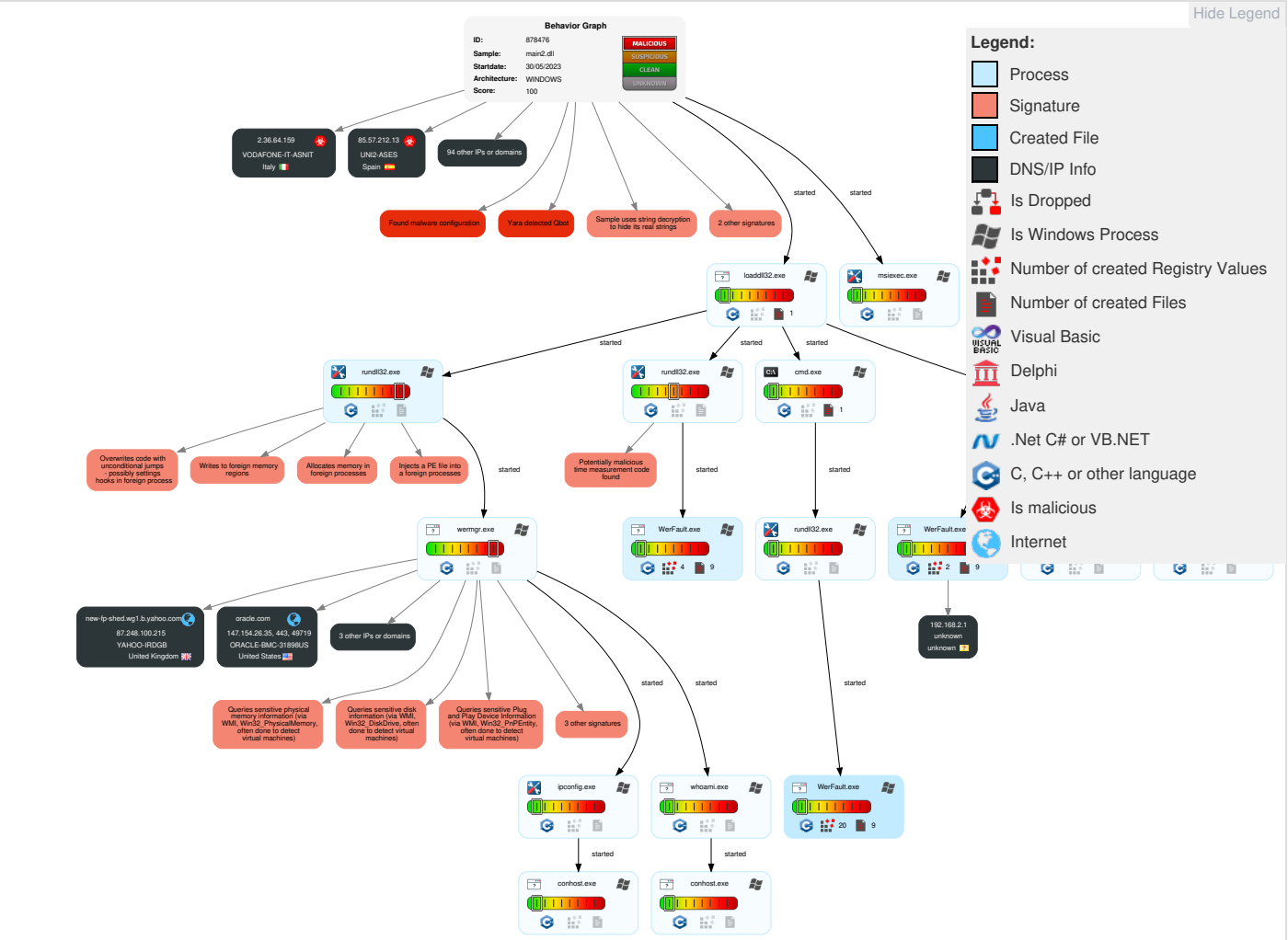
Yara detected Qbot

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 Masquerading	1 Credential API Hooking	2 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	2 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 6 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 1 Process Injection	Security Account Manager	3 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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

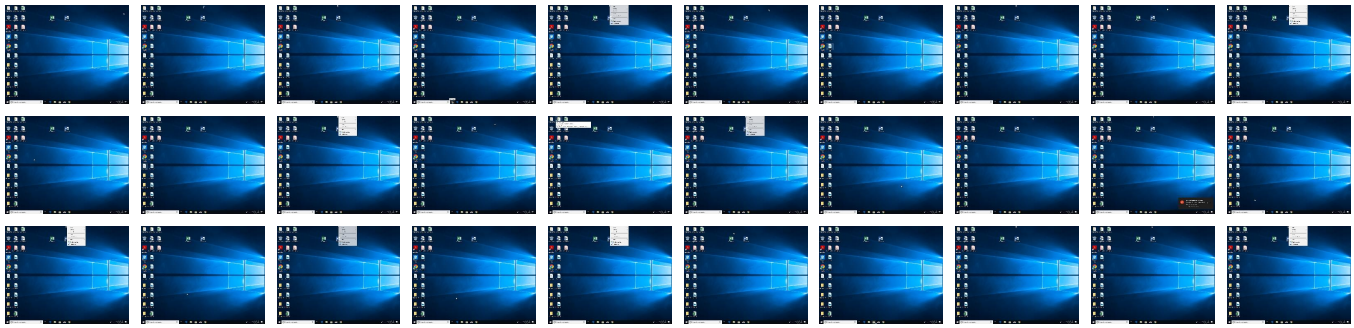
Behavior Graph

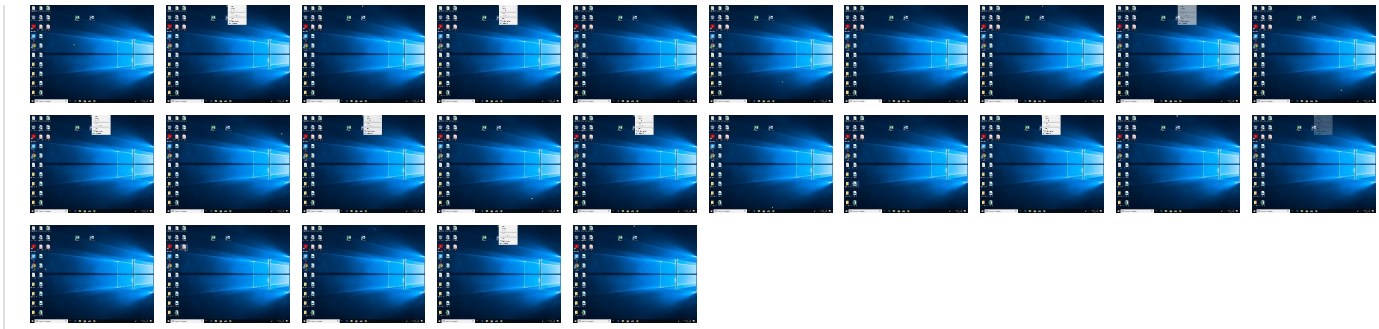


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
main2.dll	0%	ReversingLabs		
main2.dll	3%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://s2.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://s2.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	URL Reputation	safe	
http://https://s.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://dc.oracleinfinity.io	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Virustotal		Browse
http://https://dc.oracleinfinity.io	0%	Virustotal		Browse
http://https://c.go-mpulse.net	0%	Virustotal		Browse
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Avira URL Cloud	safe	
http://https://d.oracleinfinity.io	0%	Avira URL Cloud	safe	
http://https://c.go-mpulse.net	0%	Avira URL Cloud	safe	
http://https://s.go-mpulse.net	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	0%	Avira URL Cloud	safe	
http://https://d.oracleinfinity.io	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
new-fp-shed.wg1.b.yahoo.com	87.248.100.215	true	false		high
oracle.com	147.154.26.35	true	false		high
yahoo.com	54.161.105.65	true	false		high
www.yahoo.com	unknown	unknown	false		high
www.oracle.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://yahoo.com/	false		high
http://https://oracle.com/	false		high
http://www.yahoo.com/	false		high
http://https://www.yahoo.com/	false		high

URLs from Memory and Binaries

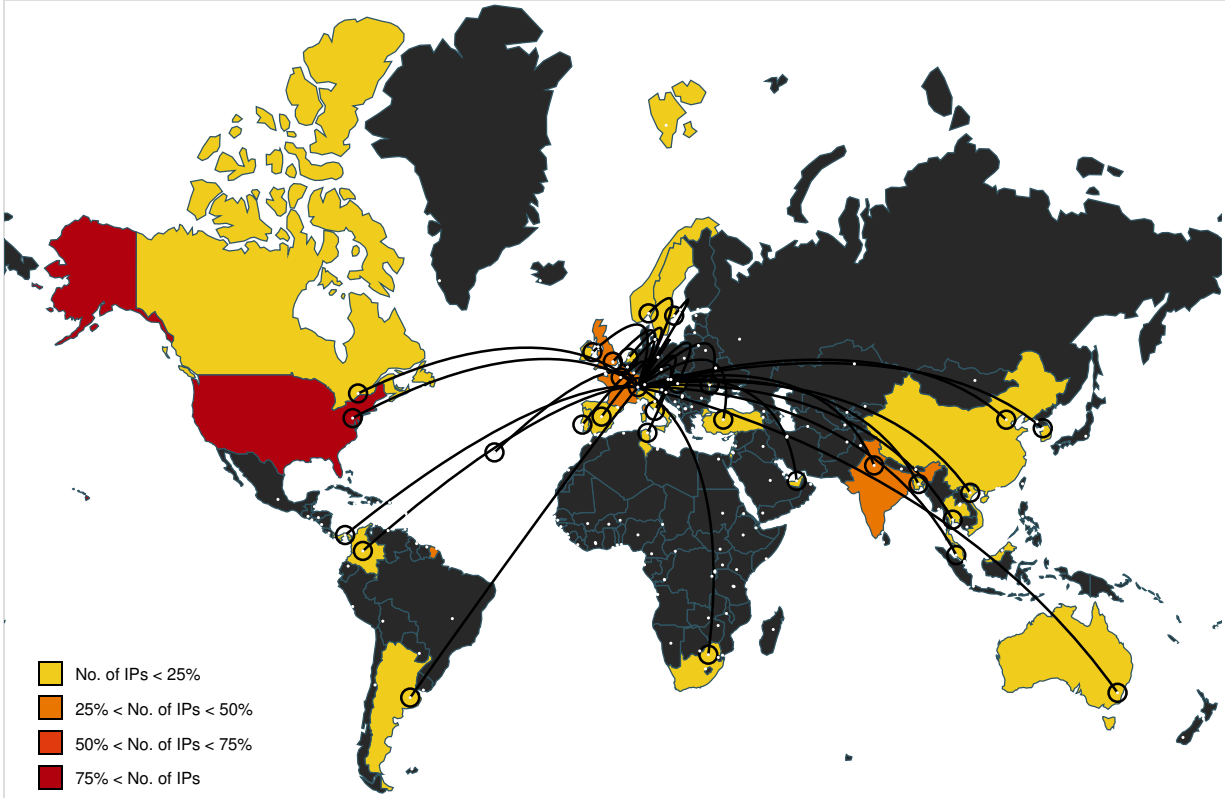
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/ss/rapid-3.53.38.js	TBWYS6DL.htm.24.dr	false		high
http://https://s.yimg.com/cx/pv/perf-vitals_3.1.0.js	TBWYS6DL.htm.24.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/mSue5SVNN_TGu6vhxeFaIQ--~B/Zmk9c3RyaW07aD0zODg7cT05NTt3PTcyMDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://s.yimg.com/aaq/spotim/	TBWYS6DL.htm.24.dr	false		high
http://https://s2.go-mpulse.net/boomerang/	upgrade-browser[1].htm.24.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://developer.oracle.com/	upgrade-browser[1].htm.24.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uu/api/res/1.2/k6Yan1hmgAcQ_.RyIRyjKA--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://tags.tiqcdn.com/	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/asset/web/fonts/redwoodicons.woff2	upgrade-browser[1].htm.24.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/JB3oERIZNZLPfu6X4e9z6A--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://consent.trustarc.com	upgrade-browser[1].htm.24.dr	false		high
http://https://fp-graviton-home-gateway.media.yahoo.com/	TBWYS6DL.htm.24.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/gQ4w2GlaUg5XgxXVq6fU_w--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://6.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830441%7C0%7C225%7CAdId=11101911;BnId=2;ct=2070467	TBWYS6DL.htm.24.dr	false		high
http://https://openweb.jac.yahoosandbox.com	TBWYS6DL.htm.24.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/iqJCDdqoBvMFTq393T2TJw--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://www.oracle.com/asset/web/favicons/favicon-192.png	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/upgrade-browser/	upgrade-browser[1].htm.24.dr	false		high
http://https://d.oracleinfinity.io	upgrade-browser[1].htm.24.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	TBWYS6DL.htm.24.dr	false	• URL Reputation: safe	unknown
http://https://www.oracle.com/asset/web/fonts/oraclesansvf.woff2	upgrade-browser[1].htm.24.dr	false		high
http://https://academy.oracle.com/en/oa-web-overview.html	upgrade-browser[1].htm.24.dr	false		high
http://https://s.go-mpulse.net/boomerang/	upgrade-browser[1].htm.24.dr	false	• URL Reputation: safe	unknown
http://https://investor.oracle.com/home/default.aspx	upgrade-browser[1].htm.24.dr	false		high
http://https://search.yahoo.com/search?p=	TBWYS6DL.htm.24.dr	false		high
http://https://www.google.com/chrome/	upgrade-browser[1].htm.24.dr	false		high
http://schema.org	TBWYS6DL.htm.24.dr	false		high
http://www.opensource.org/licenses/mit-license.php	TBWYS6DL.htm.24.dr	false		high
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html"	TBWYS6DL.htm.24.dr	false		high
http://https://tms.oracle.com/	upgrade-browser[1].htm.24.dr	false		high
http://https://streams.videolan.org/upload/	rundll32.exe, rundll32.exe, 00000003.00000002.397004221.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000004.00000002.396807812.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 0000000B.00000002.397912264.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 0000000E.00000002.403828538.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000010.00000002.403924060.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000011.00000002.409420276.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, main2.dll	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uu/api/res/1.2/QfDZyyWWOuopF7byq4JOPw--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://developer.oracle.com/community/events/devlive-level-up-march-2023-recordings.html	upgrade-browser[1].htm.24.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/.qI7oCjOo8kDU9oJt_JGgg--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://twitter.com/oracle	upgrade-browser[1].htm.24.dr	false		high
http://https://www.youtube.com/oracle/	upgrade-browser[1].htm.24.dr	false		high
http://https://c.go-mpulse.net	upgrade-browser[1].htm.24.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/aaq/nel/js/spotIm.custom.SpotIMJAC.modal.9d3270fa67932556c75baaed2c09c955.js	TBWYS6DL.htm.24.dr	false		high
http://https://dc.oracleinfinity.io	upgrade-browser[1].htm.24.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/aaq/hc/homepage-pwa-defer-1.1.6.js	TBWYS6DL.htm.24.dr	false		high
http://https://www.oracle.com/corporate/accessibility/	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/asset/web/favicons/favicon-128.png	upgrade-browser[1].htm.24.dr	false		high
http://https://tms.oracle.com/main/prod/utag.js	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/asset/web/favicons/favicon-32.png	upgrade-browser[1].htm.24.dr	false		high
http://https://s.yimg.com/aaq/vzm/cs_1.4.0.js	TBWYS6DL.htm.24.dr	false		high
http://https://search.oracle.com/events?q=&lang=english	upgrade-browser[1].htm.24.dr	false		high
http://https://tms.oracle.com/main/prod/utag.sync.js	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/asset/web/favicons/favicon-152.png	upgrade-browser[1].htm.24.dr	false		high
http://upx.sf.net	Amcache.hve.8.dr	false		high
http://https://developer.oracle.com/python/what-is-python/	upgrade-browser[1].htm.24.dr	false		high
http://https://s.yimg.com/uc/sf/0.1.322/js/safe.min.js	TBWYS6DL.htm.24.dr	false		high
http://https://www.yahoo.com/px.gif	TBWYS6DL.htm.24.dr	false		high
http://https://www.oracle.com/	upgrade-browser[1].htm.24.dr	false		high
http://https://oracle.112.2o7.net	upgrade-browser[1].htm.24.dr	false		high
http://https://go.oracle.com/subscriptions	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/asset/web/favicons/favicon-180.png	upgrade-browser[1].htm.24.dr	false		high
http://https://6.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830424%7C0%7C0%7CAdId=-41;BnId=0;ct=2070467765;st=	TBWYS6DL.htm.24.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-core-1.63.0.js	TBWYS6DL.htm.24.dr	false		high
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	TBWYS6DL.htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/_thhUXx96QwnlqajJOOzag--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	TBWYS6DL.htm.24.dr	false		high
http://https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	TBWYS6DL.htm.24.dr	false		high
http://https://profile.oracle.com/myprofile/account/create-account.jspx	upgrade-browser[1].htm.24.dr	false		high
http://https://tms.oracle.com/main/dev/utag.js	upgrade-browser[1].htm.24.dr	false		high
http://https://www.linkedin.com/company/oracle/	upgrade-browser[1].htm.24.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yep.video.yahoo.com/oath/js/1/oath-player.js?ypv=8.5.43&lang=en-US	TBWYS6DL.htm.24.dr	false		high
http://https://blogs.oracle.com/	upgrade-browser[1].htm.24.dr	false		high
http://https://www.oracle.com/asset/web/favicons/favicon-120.png	upgrade-browser[1].htm.24.dr	false		high
http://https://s.go-mpulse.net	upgrade-browser[1].htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.oracle.com/webapps/redirect/signon?nexturl=	upgrade-browser[1].htm.24.dr	false		high
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	TBWYS6DL.htm.24.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.82.8.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
75.143.236.149	unknown	United States		20115	CHARTER-20115US	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
86.195.14.72	unknown	France		3215	FranceTelecom-OrangeFR	true
84.215.202.8	unknown	Norway		41164	GET-NOGETNorwayNO	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
105.184.103.97	unknown	South Africa		37457	Telkom-InternetZA	true
92.186.69.229	unknown	France		12479	UNI2-ASES	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.154.26.35	oracle.com	United States		31898	ORACLE-BMC-31898US	false
84.108.200.161	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
73.29.92.128	unknown	United States		7922	COMCAST-7922US	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
82.131.141.209	unknown	Hungary		20845	DIGICABLEHU	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
86.176.144.234	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
78.92.133.215	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
88.126.94.4	unknown	France		12322	PROXADFR	true
51.14.29.227	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
81.111.108.123	unknown	United Kingdom		5089	NTLGB	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
86.132.236.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
70.112.206.5	unknown	United States		11427	TWC-11427-TEXASUS	true
41.228.224.161	unknown	Tunisia		37693	TUNISIANATN	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
102.159.188.125	unknown	Tunisia		37705	TOPNETTN	true
54.161.105.65	yahoo.com	United States		14618	AMAZON-AESUS	false
151.65.167.77	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
87.248.100.215	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
89.36.206.69	unknown	Italy		48544	TECNOADSL-ASIT	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
85.104.105.67	unknown	Turkey		9121	TTNETTR	true
94.207.104.225	unknown	United Arab Emirates		15802	DU-AS1AE	true
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
78.18.105.11	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
103.144.201.56	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
98.145.23.67	unknown	United States		20001	TWC-20001-PACWESTUS	true
82.125.44.236	unknown	France		3215	FranceTelecom-OrangeFR	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
90.78.147.141	unknown	France		3215	FranceTelecom-OrangeFR	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
213.64.33.61	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
78.160.146.127	unknown	Turkey		9121	TTNETTR	true
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
24.198.114.130	unknown	United States		11351	TWC-11351-NORTHEASTUS	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878476
Start date and time:	2023-05-30 18:08:34 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 26s
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:	35
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:	main2.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@38/27@4/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 11.5% (good quality ratio 9.1%) • Quality average: 59.4% • Quality standard deviation: 38.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 104.77.20.136, 209.197.3.8
- Excluded domains from analysis (whitelisted): e2581.dscx.akamaiedge.net, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, watson.telemetry.microsoft.com, ds-www.oracle.com.edgekey.net, wu-bg-shim.trafficmanager.net
- Execution Graph export aborted for target rundll32.exe, PID 7424 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
18:09:44	API Interceptor	5x Sleep call for process: WerFault.exe modified
18:09:45	API Interceptor	1x Sleep call for process: loaddll32.exe modified
18:09:56	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_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d05b9a9\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):	0.9052135014490089
Encrypted:	false
SSDEEP:	192:FxXkiR0oXfvHBUZMX4jed+2g/u7syS274ltWc:rkifXfvBUZMX4je1g/u7syX4ltWc
MD5:	B9EDFA472BD5749D13A25CB8333FF192
SHA1:	1C0E4A8F97358C5F4B12A5B6283100227DC46B06
SHA-256:	4ECAA43D5F351137BD6D73A82CCCFE5FD62C6C4DF8B39A678932E6B396856D90
SHA-512:	7EAAC264DC1BDBC8A43D0EA0AC591A14A3045B25C7C418DF61B88DE901657549228ED934B9F8F95424EA00C4934125508CFBFE0EB5DB09A9D396697F9FEE8310
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.9.9.6.8.9.7.6.9.0.7.1.0.3.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.8.9.7.8.0.6.3.3.3.9.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.e.c.c.c.d.4.6.-.f.7.3.b.-.4.2.2.f.-.9.0.3.7.-.7.8.a.e.1.4.1.5.2.f.0.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.1.0.4.1.7.3.d.-.f.6.8.7.-.4.4.9.7.-.9.9.4.1.-.6.6.c.6.c.9.f.8.7.1.4.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.d.0.c.-.0.0.0.1.-.0.0.1.f.-.e.3.8.1.-.a.1.9.0.5.c.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d1db9c8\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):	0.9052658857422392
Encrypted:	false
SSDEEP:	192:Zkic0oXOvHBUZMX4jed+2g/u7syS274ltWc:Wi6XOvBUZMX4je1g/u7syX4ltWc
MD5:	A528D939BE37BB0B63072E494AE00B7D
SHA1:	BF049338C874181C7566F5F02B0FFA167F0196F9

SHA-256:	5D14E29AA4577D675F6C714995B4636998D38CDF5326D3FDAC18A9A12A309974
SHA-512:	8B0183799B8372DC28F04386BF61DF64E962A74FB6ED63C66B9ED23185C695C1BD45E6D14EFA49A98FFDA6A390483E809B8D6AFE4809F5643548D96C74188D4
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.9.9.6.8.9.7.6.8.8.2.8.2.4.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.8.9.7.8.0.8.5.9.4.0.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.7.e.5.f.9.7.5.-.a.e.6.5.-.4.e.b.e.-.8.e.a.4.-.c.0.5.9.2.a.1.b.d.0.9.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.e.c.7.7.0.8.8.-.e.4.7.f.-.4.7.7.2.-.a.c.f.4.-.2.0.a.4.f.a.3.4.0.1.f.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.d.0.0.-.0.0.0.1.-.0.0.1.f.-.e.d.a.a.-.9.1.9.0.5.c.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1e81c6c8\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):	0.9048717935519408
Encrypted:	false
SSDEEP:	192:JwzKDi40oXwvHBUZMX4jed+2g/u7sySZ74ltWce:JUKDi+XwvBUZMX4je1g/u7syX4ltWc
MD5:	619C74AB616171DE26F2EA2A354138B4
SHA1:	E6CBB8433F8851A4892955AA09A6C63D7EE3A8EB
SHA-256:	29A0B89F8A507C11B43D8CEF751B324BCAD7F780DFB8BCE9C9D711868D423B58
SHA-512:	CEF3BACEA5CD867B7B9E611227833A5D8C5C555C711422512B375530D67AE36485C54326425FE9067A2AE4CD2156F3227A365D04373FC04BC3CACDC895176421
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.9.9.6.8.9.8.6.2.1.2.0.2.4.1.....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.=.1.3.3.2.9.9.6.8.9.8.7.3.0.5.7.9.5.0.....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.=.c.b.4.2.f.f.4.d.-.9.2.b.1.-.4.3.2.0.-.a.2.2.1.-.b.7.b.e.e.e.f.1.0.0.6.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.f.e.9.2.3.9.8.-.a.0.4.4.-.4.d.a.2.-.a.8.f.2.-.a.6.6.c.5.4.2.6.9.b.b.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.e.5.8.-.0.0.0.1.-.0.0.1.f.-.1.6.c.e.-.0.6.9.6.5.c.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e71ba64\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):	0.9050349244255587
Encrypted:	false
SSDEEP:	192:MKji30oX8zHBUZMX4jed+2g/u7sySZ74ltWc:tjiJX8zBUZMX4je1g/u7syX4ltWc
MD5:	AD88D206EBFAD6561E03AFE5DF25F581
SHA1:	55A1A630382260429208 32DE9D2C996244360729
SHA-256:	B1B35FB04332CED82D406D99DEFCACB904904233E02EAD23A96B3879A473C160
SHA-512:	3D06A01736F2D15B79312265CBDA738AD604B42FC606A77A70B2ABE4F4FBF76A2E83AE38B81EF2ECF4A48C1A7F4424B1E586B874BA96A933E82F98A049BE83EF
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.9.9.6.8.9.8.2.2.5.3.5.7.9.2.....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.=.1.3.3.2.9.9.6.8.9.8.3.0.6.6.0.5.7.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.3.f.7.0.0.b.a.-.7.d.c.8.-.4.f.1.0.-.9.8.3.3.-.9.7.1.2.5.8.1.a.c.5.2.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.4.3.2.4.6.9.6.-.7.7.2.3.-.4.1.f.a.-.a.0.e.7.-.1.7.9.b.5.b.6.9.b.5.1.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.d.f.8.-.0.0.0.1.-.0.0.1.f.-.2.6.0.4.-.3.3.9.4.5.c.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e91c745\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):	0.9053566417919718
Encrypted:	false
SSDEEP:	192:nrkie0oXpzHBUZMX4jed+2g/u7sySZ74ltWc:lioXpzBUZMX4je1g/u7syX4ltWc
MD5:	BADF4E4B2B1FA3D0A73B9257E0F5540A

SHA1:	388E0B053DD46299573E210463D3161CA261AA45
SHA-256:	52BD72F7FECB8EC5E5587670E1068AE98B93E81AE347AB92674AB5DB16F6DCD7
SHA-512:	379AF1768D59BA0322B7ACC682BC0BBA758A63CA885C96410B784FE0F2B37D3704EA3C651899D0EE31FA8DB6DE10D4A31DC1A0C2ECADA1B52CC303FD21DE D90E
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.9.9.6.8.9.8.6.2.8.6.1.0.9.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.8.9.8.7.3.9.5.4.7.7.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.e.a.6.c.4.8.9.-.3.0.7.e.-.4.e.0.d.-.b.8.6.2.-.8.9.5.c.1. d.3.c.5.9.b.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.7.2.1.f.4.c.c.-.6.e.8.c.-.4.8.6.1.-.b.4.c.2.-.9.1.c.1.8.8.4.b.8.2.d.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.e.8.0.- .0.0.0.1.-.0.0.1.f.-.d.9.7.5.-.2.9.9.6.5.c.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 01:09:37 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37064
Entropy (8bit):	2.3096101392918698
Encrypted:	false
SSDEEP:	192:chZHZ53+T+VABO5SkbRyvS00t7XEZ0s1KAzQr08T2Xnn:OU++05LbRyvQ78Qr0Z
MD5:	E3E4BD791FBC644C198DB3A8BD99D51D
SHA1:	101E79CD20CDD200EB24B1203299FE443284721A
SHA-256:	8278CD4BCFCC32FD3840B4E746F05A396F3F75B265892BF30020DE88609220CE
SHA-512:	FCB029EE894AD36EBA040E4C705F0DDD640BE9094E2E459F7A6EE5760858FDFB5829D1797005D7FBC4486EB0F43CA3E8B2D2FE2E003445FB13BCDC45E08149 F0
Malicious:	false
Preview:	MDMP..... .....Q.vd.....d.....l.....)..... T.....8..... T.....v.....U.....B.....GenuineIn telW..... T.....O.vd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 01:09:37 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38852
Entropy (8bit):	2.210160967168378
Encrypted:	false
SSDEEP:	192:cgiHZ53+T+MSVO5SkbR8d28JYUS7eyzNqhSpn6u:+U+345LbR8dhHSzZ
MD5:	ECA4105B05EF5789BF8736421FB258B2
SHA1:	BE90EA377A0A18556CE90E961EE996BC21F36023
SHA-256:	2E545BFF08F0C9C7A1A1E46FF9B4D797701EE1408B6AC8A5B90E506C28C44C71
SHA-512:	F03BCF70BCCC0637862E0DADC9D258DA7A3451D770F155AFE7E5FF685E6278E1575F7C4EC5D7499A9B9652D1721430F4A31B1651370D87C1CFE10D98253E50E
Malicious:	false
Preview:	MDMP..... .....Q.vd.....d.....l.....)..... T.....8..... T.....P...t}.....U.....B.....GenuineIn telW..... T.....O.vd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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):	3.6870478208710113
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYf67Nk6Yu/6zrgmfTdkSYCpru89bKasfqum:RrlsNiw6y6YW6/gmfTdkSHK5fK
MD5:	EF7B10334288549F75D2BB4A100A469F
SHA1:	6C65E5560B7BA1F37AEB4AB684AC752AB515F864
SHA-256:	741A2125ED65F10D2264ABE36914E6C5E99F2F40C33646C2A10C442C002E166A
SHA-512:	6B2847060A2DE376245E1492446800B523144DEF61D42823A4D7636D913BA8D4FB322EBA558CEE688DB13CF0C2F78963E2078B89F9289CD6B55B95F708EF8C6C

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.>.7.4.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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):	8242
Entropy (8bit):	3.688124234999727
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7e67Nj6Y/T6ggmfTdkSYCpr189bKosfQXTum:RrlsNiS616Y76ggmfTdkSCKbfQj
MD5:	F171D2A29A70A814B59C63EC9BD50031
SHA1:	E016B2F75D586A8AEC6C13FD6772BAC539A8E2F8
SHA-256:	9928E9FE1E0AC97DE982F4722A3C0F3AD4EE8B277E4764559F9D93BA8681E013
SHA-512:	3F6B568177B3B6EC1DE9232BE105D9CD25DA6CF04B2470083830F5CEE95BF6B46B594F3F49F453D5C7C085D1E28D9A23356FBBE1D62FAAD8AAB182E20104E94C
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.>.7.4.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CEB.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4628
Entropy (8bit):	4.447467288901837
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6BiJgtWI93/Wgc8sqYjub8fm8M4JCdsIFy+q8/+B4SrSUd:uITf6Bw4ugrsqYCYJFZDWUd
MD5:	333ACBA2F3AA620458F4B13CEBAC79D4
SHA1:	BC0C46FAC2C44DE1A663A7448190157424E36320
SHA-256:	4BE930DC50DE9771BF1BBF0E8874B595345A944D14FF9ACC2AA60E58CC766DF1
SHA-512:	8925A0F53FF68A6612DE158BBA7FB8227F2457363F691728A6624CAD471BA2473FD709233C7DF74824525112E8923BC2AD376BB77CEE7FDB0A6116B8AC379FFD
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="2064140" />.. <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\WER9CFB.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4628
Entropy (8bit):	4.451853463078934
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6BiJgtWI93/Wgc8sqYjt8fm8M4JCdsIFMlF+q8/+A4SrSvd:uITf6Bw4ugrsqYOJlF4DWvd
MD5:	741BBFDEFB452D2045C53A09FE5F6B19
SHA1:	7F96F9A95B2AAA68491932DB5497E3A0A30A5E7A
SHA-256:	E31A1D2A47C364CAA986E809CD62E835386921CA4D76DA8BE7242848498DF764
SHA-512:	63BEC531C4F850F1EBCDEE149BFE10F88FECB3BC796DB84FF8D920797F762008FC3D1C00F19309842462E90FB8AB40ABF23D6794C089CCB1F6703D5B42A5A7B5
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="2064140" />.. <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\WERAFA6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 01:09:42 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37408
Entropy (8bit):	2.2622210699430085
Encrypted:	false
SSDEEP:	192:31OHZ53+T+WpDO5SkbR3biaIWqpA3USJvX8md8c2bO:8U+065LbR3h9k48mU
MD5:	7D55866986B12B11C0F1832E4F8474BC
SHA1:	C940BC9CFC14B012EFCE7D8CA03C7F0A30D698C4
SHA-256:	B5BF0CE1C9CC1820E9C7F01A8BFB0A0CD93A31315C560817036C4920A29BD5B8
SHA-512:	6978F3C44F80E240FECE5078E91289647AEABDC922C19F84619071DF3895BE966166F6AC22CB9A4EDA5806501E3DEB414FBB61A0C23AD9D8936CDAED122D38D
Malicious:	false
Preview:	MDMP..... .....V.vd.....d.....l.....)..... T.....8..... T..... x..... U..... B..... GenuineIntelW..... T..... U.vd..... 0..=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8246
Entropy (8bit):	3.6885593071576137
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJM67NA6Yuu6NEgmfTdASYCpr+89bAysfggm:RrlsNii626YX6ugmfTdAS3Axf+
MD5:	47F2BBCE9B3D03859898C7531316FDEF
SHA1:	C4613731B9DFA523A5123AB332A0E95C1D1ABD27
SHA-256:	6D00FC85A1D91F719A59FEAD76A4D1ABB2E618E052EFED793C72824C78BB0867
SHA-512:	74C45DE0C560B03AC637395EDFB22FB4D88BCFC77DCDE3C51829B95E3E535C0FB9D90BB16A76753509CC3F1A8A1EC9D6CF25D8CFD243BBAC4C4D647511DEB48F
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.>.7.6.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4628
Entropy (8bit):	4.455154617516187
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6BiJgtWI93/Wgc8sqYjp8fm8M4JCds+tFbll+q8/g61n4SrSZd:uITf6Bw4ugrsqYKJ4TGE1nDWZd
MD5:	5D32A36EC0E334CC9BA2C8A05F2D408B
SHA1:	07942D40B07312003916053F8D6E497C3EE1B734
SHA-256:	E209CFD967605A0B8F8BC3A39730BAEA6E230EAD4E7F9D8402ACA1CD5E08E624
SHA-512:	3047B79978887B1FC55E360E25482272A7836517084738BDA477C2E2A6BBC42FD4D31B77044A19516DC2040A13527E2DDFCDF1A48D39FEA6CF45D147362F4AA5
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="2064140" />.. <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\WERBF27.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 01:09:46 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43128
Entropy (8bit):	2.130821071594553
Encrypted:	false
SSDEEP:	192:jhwp3Cm6IO5SkbRtZpDXng+dUSQ5zKE9gPsXq2:3XP5LbRxDgqUFKg
MD5:	D22F0A51CA6F1D401ED7EEFD7F8ADCC0
SHA1:	6F2AE24859C11E18CEE06744282B2F099DD9B6B9
SHA-256:	0E3E37FB8F782D1D759E5F0DA008DFAF32A4CC5FED4637F0E4DE27DA79BD87DE
SHA-512:	7388E5B01A2F567FEC8A75CEA51E89A6C2D4C441F64F86A66CA4A3A6781BB74CD818816143C3AEF8A46CABE101BCCCB618E3EAEC285E37765BD604F7FE19AD22
Malicious:	false
Preview:	MDMP..... .....Z.vd.....,.....T.....8.....T.....x.....0.....U.....B.....GenuineIntelW.....T.....X...X.vd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF65.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 01:09:46 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	45212
Entropy (8bit):	2.0558254031833574
Encrypted:	false
SSDEEP:	192:jtTz3CgOO5SkbRGrCYg3GrhQHqkLhaO4SyRwEb5RwU6SM7+DfH5u:ck5LbRGrCYg2rhQHtsO4vwEb5RUSFH5
MD5:	311BBD33C2E88530FB5C59AD91FD85A8
SHA1:	F933EB67EE5F874BCB800D649F088AE4D61C5AFD
SHA-256:	FF2750FD6F0C7AB1574A0C6EF5E295C96F75E8FC9C7902CC2D8ED6AF42059520
SHA-512:	D83D6E11B25CE9394C3EAB6E616456AC6CB3AFF516D2D2834E723AD12D2CFD8AF418C7BEB51C6000EFA2B7501C2A865249CC69773DEA40B2E99C74776910FF8
Malicious:	false
Preview:	MDMP..... .....Z.vd.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....X.vd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0AF.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):	8238
Entropy (8bit):	3.6871730621914076
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirY6a6Y+k6GogmfTdkSYCprp89bkMsfwmsm:RrlsNiE6a6YF6GogmfTdkSmkffwE
MD5:	6F16A98EAE37F3A18C3EDD7EF437CA2F
SHA1:	793408DBBA112DAC705C96675E37C593D42E01ED
SHA-256:	ACEE5041695F0CC8F6A977F728D6853F71FC3F6567E8A45BB489CB33E6DD96FE
SHA-512:	8FB8032EC793B35ADA6587FDACB47AA8C419BAA0E82885E1ECF0EC51032A899A198FB9220BDD931708DF6EC684C6A0D49E8807E8D28D8A76D972E492D0C43A6B
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.>.7.7.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0FD.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):	8238
Entropy (8bit):	3.6868773202693377
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiab6Qut6Y+c6GogmfTdASYCprp89bk7sf/sm:RrlsNi26r6YN6GogmfTdASmkAfR
MD5:	BAC06276F41DFF04AA859A4C42A5B120
SHA1:	153A1082787D99DC8404EFE2B12B5C66CEF91983
SHA-256:	6DF53A487A855EF9B55281662BDA224218A71EF6976E1B2CF80D9E3AFA6D534E
SHA-512:	B3BB476B7EB3D12B2142CE10B5CA6987EA833453E471D20A3B5F8BBA3159EED36348170CCE2D54F48A804E839BD33D0B7DCF5196AE9FBE37A13B2A5AF1BA0FD2
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.>.7.8.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC11D.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4628
Entropy (8bit):	4.451377822360704
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6BiJgtWI93/Wgc8sqYjc8fm8M4JCdsIFNr+q8/+qI4SrSld:uITf6Bw4ugrsqYdJeriIDWld
MD5:	CD2F11DFDC1CC166D93DE7F644C58B24
SHA1:	41C8933E2C9C1DD2B10CD33A5F4F33F9F590C66A
SHA-256:	EE4171F361F9AC0322B7C5605869615989E61418B1A679EE87F973C4BA3A6947
SHA-512:	D9520C5602DEB263F0A94801E82E2756EED5BBBEE3C921E06658DDD3F8839DC8199D823146ED7642C4320D9787255C973F4C4E9810E9B6D3C500A80664EE116
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="2064140" />.. <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\WERC15B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4628
Entropy (8bit):	4.452843591712963
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6BiJgtWI93/Wgc8sqYj08fm8M4JCds+tFb+q8/g6E4SrSVd:uITf6Bw4ugrsqYNJ4zEEDWVd
MD5:	8D05BD8117A1BEB2A883D3A600CF2A37
SHA1:	68A348E1842681841B6DAA5AA93CCF497C452DFD
SHA-256:	7064AC427D5DDAEC6856066D36E3971DE24E274EF47E9531BC391A7A55314ED2
SHA-512:	1FC0308193DF5C5C90A99697DA02AF48564637D7A750D097FEE7D64700203AC84CB7699A8EA7993005A99BF06E7E0F2AC43062993685BFD37E2A3E15B68D25FE
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="2064140" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

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

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

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.099772979987373
Encrypted:	false
SSDEEP:	6:kKnFN+SkQlPlEGYRMY9z+4KlDA3RUeg/U3lWQy:P2kPlE99SNxAhUe7oQy
MD5:	26A3FD90F319ECED333295A2325FC4BD
SHA1:	9BC53A41871F171BAEF02727299C34FD5BF9A998
SHA-256:	478B1EF58AC2C404AFA42D6E2E989FE9F070EEE76AF7CACFF32F84F043F7076D
SHA-512:	B38ACE55CC3F5DFE7F7F763EE0F66DFC80325DB920CE66532E9EC8943E086EE211C723048F80E9A37FF7C5B9796B05709A019025B1FE3D474107CAAA681FDF7B
Malicious:	false
Preview:	p..... .....6w.T]...(..... .....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\TBWYS6DL.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, ASCII text, with very long lines (64945)
Category:	modified
Size (bytes):	858019
Entropy (8bit):	5.568419032494789
Encrypted:	false
SSDEEP:	6144:ZwYjR8Cd18F3OYRKBfDWptCLhQtICvOHXQ4YdZatRNCleiUaII6rD5wAC:Z9R8t3OYc8p0WOHA4Ri06rD5wAC
MD5:	A310B1F45AAED275DCAAF7E068257E44
SHA1:	84E571948BDBD06274B5741A6B0BEBC5D3457A64
SHA-256:	61E5372D29CDAC32F86EB7DD38A1EDD341D239D99211EEC814D2BD9337D1CE39
SHA-512:	21B85B137A6417A969A30961308336D8D7381EA4D6B1F80C2D7D997F13A08D11C077A5F0A6DD2D063E8AFD790EF301BC43DC7BA82FB20B86D7325A7901B4B85
Malicious:	false
Preview:	<!doctype html><html id=atomic class="ltr desktop-lite fp fp-none bkt900 ua-ie ua-11.0" lang=en-US data-color-scheme><head><script nonce=feef228727d1bcff543fbf1c3b26a2d457363daacaad78c949db39706364fa81>. window.performance.mark('PageStart');. document.documentElement.className += ' JsEnabled jsenabled';. /**. * Empty darlaOnready method, to avoid JS error.. * This can happen when Async Darla JS file is loaded earlier than Darla Proxy JS.. * This method will be overridden by Darla Proxy. */. window.darlaOnready = function() {};. </script><title>Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos</title><meta http-equiv=content-type content="text/html; charset=utf-8"><meta http-equiv=x-dns-prefetch-control content=on><meta http-equiv=X-UA-Compatible content=chrome=1><meta name=description content="Latest news coverage, email, free stock quotes, live scores and video are just the beginning. Discover m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\t5[1]	
Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	ASCII text, with very long lines (1000), with no line terminators
Category:	dropped
Size (bytes):	1000
Entropy (8bit):	5.950009487715204
Encrypted:	false
SSDEEP:	24:gM1SxchN3TJvshx7CJxhxZbnIyejSv/uX2jMJen4:doxc3N6xqBZbnIu+X24Jen4
MD5:	F504DE218DE9DDC1C53FE50B5B8BD411
SHA1:	50634F346F2260588D4967B8A19AA8AF92E7968D
SHA-256:	64513A1465565A58EA7C4DDF8BFEBDEDAE7CD3D0083F47B6EDB8D6E04819A184
SHA-512:	DBB9E88CA35501ABF1E9827A38D7005450708E12AF16C940AE9327A6376BEF79693259AA855091B782F335B772130A7A592C786202E34FDB699490534E59D43B
Malicious:	false
Preview:	w63fyi7lllp1ok5XWpK7kXbBu7MQ3at1ySX8zalGLLKP7hK/C/lGeALgttrPIIBJswRPtzReY2pCDjs39FuHxj7b3fvTQ4DRmz2bs8MmOHq0FprEFG8wPYT6Y4wAfRbXhY OKmqQ/S67wwSHmz4vIMSMJiMWFcQmAvTZ9YjJX2V/OMrO7OPPrukoigfJi1GFF2kLM3qNcd408sEfHJdPRFAqO8DzI7f1XjPnSSmyWGwNkZbvKptu3BQnl+Q 0SJtknJU4Ko9l2JnxU8+Eah7G5xwGoDJ+jXvFygGpKudM3ovPsNlp1g2anDnnoEBx35zEPmyFnlyRvYslVB+oDfw9Mnilzf4XMrAnXDmVbM1XM4Dtf3hL4v27M1iAd/qfD krovt7jQx0N0DOz5eBpEVWXvhD2DerpnruNIEcYVrRGsPl4M/zW94Khs1lhms8j+VHgZ6X8rpNhy6cG4Mcfbfs/+fybNYImZCjs7vgLwbdhAtnErQ/wV2bwdLqlaE9u7GH g7DwOlCOo8WBo6eQK965X3h7B4XxyHJ+1XpoT2QAylpKy+UGNuiLg/tEs7Z8Nzlds8KnztHq54ar9sAFPsN+Hz0vMf/GecUX6RgGT0bdHIREe0p1bo3A+vj12yl7Fcj9Wl xwMKnQsy7cndLBd1RgIds+qFNL6d67hQJq49vbmvsv3/Lw17nUUSm8HjpwvnemswdW1HZmeB+S7Rz1b7Mq5ix7WAAPCJDPpAYnIHfQB0TMpW5vuc4J3/5dbj AaMdJhy4j0wd6B1mt16trNnO8OC2RSbF+Hv2i7ilqqbCqOxdHU4yIsh9gjUGDse7Hh8iLiz2kUdBgc1L/H4oj8AB9qekaB9eAzL93Hsf+/9thy5v8aebuvDSjdwKEmjWGB PqZS33dJq95BJ7+3ugENG1Edqviag2PyMdD1EbQ9XT8yn9UTk/E5hVlNB8rmnPiXqHXQfQ3cTqf5rl8bTO4W6m3sezsvY3l5sYpXZUsO3RR0w0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\upgrade-browser[1].htm	
Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (4345)
Category:	dropped
Size (bytes):	31409
Entropy (8bit):	5.484787378281497
Encrypted:	false
SSDEEP:	384:yNzvkeuRPglyav5gzR9ZzC0npYaLNC96OXoYsq5PGmDMXac6Cx3XWiHXK2JmUy8:2keuRPglpv5grbtLfSemD4x5a2J/r
MD5:	55C780C7E57A35B7E0EBC775FCE32E14
SHA1:	64538C2DEC557F0099C67E6CE59767E353D4E1C2
SHA-256:	841563D99A350645AC34C2E48E600C4B57BA75454E610630EC50F536608EDB0E
SHA-512:	2CF61ECF48E018604A12493DF0D5C6E43C1F246C6E81D1E65965BC81CAB92B5DAAF650C076D525816ACDB6AF9D00B94C406A38427E8741655ACEA4A1459CE6 B
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="en-US" class="no-js"> start : Framework/Redwood2 -->. start : ocom/common/global/components/framework/head -->.<head>. start : ocom/common/global/components/head -->.<title>Unsupported Browser | Oracle</title>.<meta name="Title" content="Unsupported Browser | Oracle">.<meta n ame="Description" content="Please upgrade to or install one of the following browsers to get to the page you.re looking for. ">.<meta name="Keywords" content="U nsupported Browser ">.<meta name="siteid" content="us">.<meta name="countryid" content="US">.<meta name="robots" content="noindex, nofollow">.<meta na me="country" content="United States">.<meta name="Language" content="en">.<meta name="Updated Date" content="2021-06-09T14:08:01Z">.<script type="text /javascript">.var pageData = pageData || {};.//page info.pageData.pageInfo = pageData.pageInfo || {};.pageData.pageInfo.language = "en";.pageData.pageInfo.country = "United States";.pageData.pageInfo.pageTitle = "Unsupport

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):	4.292897804285154
Encrypted:	false
SSDEEP:	12288:iVq64flzm6eGB7SuQFai3pr9Bzjmdcry+iHWi4efHhOJMPe+RlMQA0a:764flzm6eGB7SuGzg
MD5:	9AA8F425FCE17CC5A3A9E7D7331CCB01
SHA1:	9E81E31405FCB0D5A535651CAF67404A694B4D98
SHA-256:	BF971AE79FB7F7BADAEDE71F36EB0E984D9CAABC3632345E7EE2A6999394E49B
SHA-512:	170E540A2953A5C80022F512FE5CE4FCA40E1CF3034AFAA916A2BBC49EAAC9E07E97B57FD5CD8A373978CA9BFEAA36E2053B327A98305169968CB0A5471D76 47
Malicious:	false
Preview:	regfk...k...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.rmtmn..\..... ....r8..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.953435618454874
Encrypted:	false
SSDEEP:	384:HHe5Rftx1LrPJ4JGrtHQnoEtPJUSGl9OlrIRCMYVNZ7qEXPJ:nwRftx1XJ4J8HQoEYSC9OgMYJqE
MD5:	2866317A8F467BA647F57AC85F8D2405
SHA1:	421750DB26505A7863A14B854AEF321C674A3303
SHA-256:	5E5B5BDD32BAF5C31DEC959E572878343D0C891B17471005AA44DD17B3ADC1AD
SHA-512:	C1D868C32BD19034904DBE4030C079344488918F456D8880DA56227CD95E8D75CB67C25DDC72972F59946EE266DC30C90472DD0EF71583CC863E79C90FFBEA
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.rmtmn..\..... .....t8..HvLE.>.....j.....Z...i.n...v.....0.....hbin.....p.\..,.....nk,..*..\.....h..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ..*..\..... ....Z.....Root.....lf.....Root....nk ..*..\.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.765768694509863
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:	main2.dll
File size:	952832
MD5:	5e107608dd00957472db2c1fcc77599d
SHA1:	d9bfa3e88ca0f86182cb84d4008ac6b346b755e9
SHA256:	185737016a01e84bf88523a4681723b4f2d0d22520e77b76740cc3c6323e38bf
SHA512:	22dfae946f939eb361cef49ed6eb953097a23a31be0e97e6b7d31d3b2152c2371da44e9e6bdd369e7145856ba75369fea4deab18fa035e2a2cbd1e7d4e23caf4
SSDEEP:	24576:UkgLxg2eMP8EN8Vo7zgDQ9uo4iZSBi/u3wXqx9jKVM5qx0YJ:x/jDQMo49wpq
TLSH:	96157CC0FAD744FAE46B58B1B09AB7AFAB3016090138CD36DF658E09E977B401DDB245
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..d.....#...8..... .....@... .....hC.

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x10001390
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, 32BIT_MACHINE, DEBUG_STRIPPED, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x640DB86D [Sun Mar 12 11:33:01 2023 UTC]
TLS Callbacks:	0x1008e1a0, 0x1008e150, 0x1009f130
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:	198d27fbc9acaddaf58c47ff836570ae

Entrypoint Preview
Instruction
sub esp, 0Ch
mov dword ptr [101D66DCh], 00000000h
mov ecx, dword ptr [esp+18h]
mov edx, dword ptr [esp+14h]
mov eax, dword ptr [esp+10h]
call 00007F94E0B93457h
add esp, 0Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
nop
sub esp, 1Ch
mov eax, dword ptr [esp+20h]
mov dword ptr [esp], 100C7000h
mov dword ptr [esp+04h], eax
call 00007F94E0C2F8CEh
add esp, 1Ch
ret
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 18h
mov dword ptr [esp], 10001400h
call 00007F94E0B935D3h
leave
ret
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
nop
ret
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
push edi

Instruction
push esi
push ebx
mov edx, dword ptr [esp+14h]
mov esi, dword ptr [esp+1Ch]
mov edi, dword ptr [esp+18h]
movzx ebx, dx
shr edx, 10h
test esi, esi
je 00007F94E0B93688h
nop
cmp esi, 04h
jbe 00007F94E0B93642h
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
movzx eax, byte ptr [edi]
add edi, 04h
sub esi, 04h
movzx ebp, byte ptr [edi-03h]
movzx ecx, byte ptr [edi-02h]
add eax, ebx
movzx ebx, byte ptr [edi-01h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1d8000	0x4368	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1dd000	0x123c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1e1000	0x380	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1e2000	0x3fd8	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc4a24	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1dd2e8	0x298	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa8334	0xa8400	False	0.4476559597882615	data	6.437673909255203	IMAGE_SCN_CNT_CODE, 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_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xaa000	0x100	0x200	False	0.28125	Matlab v4 mat-file (little endian) \377\377\377\377 , text, rows 4294967295, columns 4294967295, imaginary	2.141186603235595	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	0xab000	0x1b37c	0x1b400	False	0.3674741972477064	data	5.340849609955588	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
.bss	0xc7000	0x110244	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_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
.edata	0x1d8000	0x4368	0x4400	False	0.4035500919117647	data	5.488547512980677	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
.idata	0x1dd000	0x123c	0x1400	False	0.3578125	data	5.173278625033256	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
.CRT	0x1df000	0x30	0x200	False	0.060546875	data	0.25451054171027127	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	0x1e0000	0x8	0x200	False	0.02734375	data	0.0	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
.rsrc	0x1e1000	0x1a662	0x1b000	False	0.9552589699074074	data	7.907856136101986	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	0x1fc000	0x3fd8	0x4000	False	0.72137451171875	data	6.607281543167989	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

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1e1058	0x324	data	English	United States

Imports

DLL	Import
bcrypt.dll	BCryptCloseAlgorithmProvider, BCryptGenRandom, BCryptOpenAlgorithmProvider
KERNEL32.dll	AcquireSRWLockExclusive, AddVectoredExceptionHandler, CloseHandle, CreateEventA, CreateFileMappingA, CreateSemaphoreA, DeleteCriticalSection, DuplicateHandle, EnterCriticalSection, FileTimeToSystemTime, GetConsoleMode, GetConsoleScreenBufferInfo, GetCurrentProcess, GetCurrentProcessId, GetCurrentThread, GetCurrentThreadId, GetFullPathNameW, GetHandleInformation, GetLastError, GetModuleHandleA, GetModuleHandleW, GetProcAddress, GetProcessAffinityMask, GetProcessTimes, GetStdHandle, GetSystemTimeAdjustment, GetSystemTimeAsFileTime, GetThreadContext, GetThreadPriority, GetThreadTimes, GetTickCount64, GetTimeZoneInformation, InitOnceBeginInitialize, InitOnceComplete, InitializeConditionVariable, InitializeCriticalSection, InitializeSRWLock, IsDBCSLeadByteEx, IsDebuggerPresent, LeaveCriticalSection, MapViewOfFile, MultiByteToWideChar, OpenProcess, OutputDebugStringA, QueryPerformanceCounter, QueryPerformanceFrequency, RaiseException, ReleaseSRWLockExclusive, ReleaseSemaphore, RemoveVectoredExceptionHandler, ResetEvent, ResumeThread, SetConsoleTextAttribute, SetEvent, SetLastError, SetProcessAffinityMask, SetSystemTime, SetThreadContext, SetThreadPriority, Sleep, SleepConditionVariableSRW, SuspendThread, TlsAlloc, TlsGetValue, TlsSetValue, TryEnterCriticalSection, UnmapViewOfFile, VirtualProtect, VirtualQuery, WaitForMultipleObjects, WaitForSingleObject, WaitForSingleObjectEx, WakeAllConditionVariable, WakeConditionVariable, WideCharToMultiByte, WriteConsoleW
msvcrt.dll	__mb_cur_max, __setusermatherr, _aligned_free, _aligned_malloc, _aligned_realloc, _amsg_exit, _beginthreadex, _endthreadex, _errno, _fstat64, _get_osfhandle, _gmtime64, _hypot, _initterm, _iob, _localtime64, _lock, _mktime64, _setjmp3, _sopen, _ultoa, _unlock, _wsopen, abort, acos, asin, atan, atoi, bsearch, calloc, clock, cosh, exit, fprintf, fputc, fputs, free, fwrite, getc, getenv, islower, isspace, isupper, isxdigit, localeconv, log10, malloc, memchr, memcmp, memcpy, memmove, memset, printf, rand, realloc, setlocale, sinh, strchr, strcmp, strcpy, strcspn, strerror, strftime, strlen, strncmp, strrchr, strspn, strstr, strtol, strtoul, tan, tanh, tolower, ungetc, vfprintf, wcscat, wcscpy, wcslen, longjmp, _strdup, _read, _isatty, _fdopen, _close

Exports

Name	Ordinal	Address
mv_add_i	1	0x10021110
mv_add_q	2	0x10032e70
mv_add_stable	3	0x100252f0
mv_adler32_update	4	0x10001410
mv_aes_alloc	5	0x10001bd0
mv_aes_crypt	6	0x10001bf0
mv_aes_ctr_alloc	7	0x100022f0
mv_aes_ctr_crypt	8	0x10002480
mv_aes_ctr_free	9	0x10002420
mv_aes_ctr_get_iv	10	0x10002370
mv_aes_ctr_increment_iv	11	0x10002430
mv_aes_ctr_init	12	0x100023c0
mv_aes_ctr_set_full_iv	13	0x10002340

Name	Ordinal	Address
mv_aes_ctr_set_iv	14	0x10002310
mv_aes_ctr_set_random_iv	15	0x10002380
mv_aes_init	16	0x10001c10
mv_aes_size	17	0x100ab00c
mv_append_path_component	18	0x10006eb0
mv_asprintf	19	0x10006850
mv_assert0_fpu	20	0x1008a480
mv_audio_fifo_alloc	21	0x10002670
mv_audio_fifo_drain	22	0x10002af0
mv_audio_fifo_free	23	0x10002610
mv_audio_fifo_peek	24	0x10002900
mv_audio_fifo_peek_at	25	0x10002990
mv_audio_fifo_read	26	0x10002a40
mv_audio_fifo_realloc	27	0x100027b0
mv_audio_fifo_reset	28	0x10002b70
mv_audio_fifo_size	29	0x10002bb0
mv_audio_fifo_space	30	0x10002bc0
mv_audio_fifo_write	31	0x10002850
mv_base64_decode	32	0x100076c0
mv_base64_encode	33	0x100078d0
mv_basename	34	0x10006d70
mv_blowfish_alloc	35	0x10007da0
mv_blowfish_crypt	36	0x100084b0
mv_blowfish_crypt_ecb	37	0x10007dc0
mv_blowfish_init	38	0x100a3f90
mv_bmg_get	39	0x100224c0
mv_bprint_append_data	40	0x10008f30
mv_bprint_channel_layout	41	0x1000c9f0
mv_bprint_chars	42	0x10008d20
mv_bprint_clear	43	0x10009670
mv_bprint_escape	44	0x10009730
mv_bprint_finalize	45	0x10009690
mv_bprint_get_buffer	46	0x10009500
mv_bprint_init	47	0x10008880
mv_bprint_init_for_buffer	48	0x100089a0
mv_bprint_strftime	49	0x10009130
mv_bprintf	50	0x100089c0
mv_buffer_alloc	51	0x10009dc0
mv_buffer_allocz	52	0x10009ef0
mv_buffer_create	53	0x10009e60
mv_buffer_default_free	54	0x10009d10
mv_buffer_get_opaque	55	0x1000a090
mv_buffer_get_ref_count	56	0x1000a0a0
mv_buffer_is_writable	57	0x1000a070
mv_buffer_make_writable	58	0x1000a0b0
mv_buffer_pool_buffer_get_opaque	59	0x1000a9b0
mv_buffer_pool_get	60	0x1000a720
mv_buffer_pool_init	61	0x1000a5f0
mv_buffer_pool_init2	62	0x1000a590
mv_buffer_pool_uninit	63	0x1000a650
mv_buffer_realloc	64	0x1000a1d0
mv_buffer_ref	65	0x10009fc0
mv_buffer_replace	66	0x1000a480
mv_buffer_unref	67	0x1000a000
mv_calloc	68	0x100266d0
mv_camellia_alloc	69	0x1000b0b0
mv_camellia_crypt	70	0x1000b0d0
mv_camellia_init	71	0x100a415e
mv_camellia_size	72	0x100ac650

Name	Ordinal	Address
mv_cast5_alloc	73	0x1000c090
mv_cast5_crypt	74	0x1000c1b0
mv_cast5_crypt2	75	0x1000c0b0
mv_cast5_init	76	0x100a4f3e
mv_cast5_size	77	0x100aea60
mv_channel_description	78	0x1000c470
mv_channel_description_bprint	79	0x1000c3c0
mv_channel_from_string	80	0x1000c560
mv_channel_layout_channel_from_index	81	0x1000dc10
mv_channel_layout_channel_from_string	82	0x1000eac0
mv_channel_layout_check	83	0x1000ec10
mv_channel_layout_compare	84	0x1000edb0
mv_channel_layout_copy	85	0x1000d340
mv_channel_layout_default	86	0x1000eff0
mv_channel_layout_describe	87	0x1000dba0
mv_channel_layout_describe_bprint	88	0x1000d4d0
mv_channel_layout_extract_channel	89	0x1000d060
mv_channel_layout_from_mask	90	0x1000d1b0
mv_channel_layout_from_string	91	0x1000dd40
mv_channel_layout_index_from_channel	92	0x1000e760
mv_channel_layout_index_from_string	93	0x1000e950
mv_channel_layout_standard	94	0x1000f050
mv_channel_layout_subset	95	0x1000f080
mv_channel_layout_uninit	96	0x1000d270
mv_channel_name	97	0x1000c2d0
mv_channel_name_bprint	98	0x1000c220
mv_chroma_location_enum_to_pos	99	0x10032410
mv_chroma_location_from_name	100	0x100323c0
mv_chroma_location_name	101	0x100323a0
mv_chroma_location_pos_to_enum	102	0x10032450
mv_cmp_i	103	0x100216e0
mv_color_primaries_from_name	104	0x10032270
mv_color_primaries_name	105	0x10032250
mv_color_range_from_name	106	0x10032200
mv_color_range_name	107	0x100321e0
mv_color_space_from_name	108	0x10032350
mv_color_space_name	109	0x10032330
mv_color_transfer_from_name	110	0x100322e0
mv_color_transfer_name	111	0x100322c0
mv_compare_mod	112	0x10024ed0
mv_compare_ts	113	0x10024d10
mv_content_light_metadata_alloc	114	0x10024500
mv_content_light_metadata_create_side_data	115	0x10024530
mv_cpu_count	116	0x1000f8f0
mv_cpu_force_count	117	0x1000f9e0
mv_cpu_max_align	118	0x1000f9f0
mv_crc	119	0x100101d0
mv_crc_get_table	120	0x1000fdb0
mv_crc_init	121	0x1000fbc0
mv_csp_luma_coeffs_from_avcsp	122	0x100102b0
mv_csp_primaries_desc_from_id	123	0x100102f0
mv_csp_primaries_id_from_desc	124	0x10010320
mv_d2q	125	0x10032f80
mv_d2str	126	0x100068e0
mv_default_get_category	127	0x10023720
mv_default_item_name	128	0x10023710
mv_des_alloc	129	0x10010d80
mv_des_crypt	130	0x10010e40
mv_des_init	131	0x10010da0

Name	Ordinal	Address
mv_des_mac	132	0x10010e90
mv_detection_bbox_alloc	133	0x10010ee0
mv_detection_bbox_create_side_data	134	0x10010f70
mv_dict_copy	135	0x10011d20
mv_dict_count	136	0x10011070
mv_dict_free	137	0x10011cc0
mv_dict_get	138	0x100110d0
mv_dict_get_string	139	0x100121a0
mv_dict_iterate	140	0x10011090
mv_dict_parse_string	141	0x100118c0
mv_dict_set	142	0x10011210
mv_dict_set_int	143	0x10011560
mv_dirname	144	0x10006e10
mv_display_matrix_flip	145	0x100126f0
mv_display_rotation_get	146	0x10012470
mv_display_rotation_set	147	0x100125c0
mv_div_i	148	0x100223d0
mv_div_q	149	0x10032e00
mv_dovi_alloc	150	0x10012780
mv_dovi_metadata_alloc	151	0x100127b0
mv_downmix_info_update_side_data	152	0x10012800
mv_dynamic_hdr_plus_alloc	153	0x1001d0a0
mv_dynamic_hdr_plus_create_side_data	154	0x1001d0d0
mv_dynamic_hdr_vivid_alloc	155	0x1001d130
mv_dynamic_hdr_vivid_create_side_data	156	0x1001d160
mv_dynarray2_add	157	0x10026bd0
mv_dynarray_add	158	0x10026b00
mv_dynarray_add_nofree	159	0x10026a40
mv_encryption_info_add_side_data	160	0x10012f30
mv_encryption_info_alloc	161	0x10012a70
mv_encryption_info_clone	162	0x10012b40
mv_encryption_info_free	163	0x10012cf0
mv_encryption_info_get_side_data	164	0x10012d40
mv_encryption_init_info_add_side_data	165	0x10013860
mv_encryption_init_info_alloc	166	0x10013100
mv_encryption_init_info_free	167	0x100132d0
mv_encryption_init_info_get_side_data	168	0x10013480
mv_escape	169	0x10007050
mv_expr_count_func	170	0x100176e0
mv_expr_count_vars	171	0x10017650
mv_expr_eval	172	0x100177a0
mv_expr_free	173	0x10015280
mv_expr_parse	174	0x10017110
mv_expr_parse_and_eval	175	0x100177f0
mv_fast_malloc	176	0x100271f0
mv_fast_mallocz	177	0x100272d0
mv_fast_realloc	178	0x10027140
mv_fifo_alloc	179	0x10018a20
mv_fifo_alloc2	180	0x10017e40
mv_fifo_alloc_array	181	0x10018990
mv_fifo_auto_grow_limit	182	0x10017ef0
mv_fifo_can_read	183	0x10017f10
mv_fifo_can_write	184	0x10017f40
mv_fifo_drain	185	0x100192b0
mv_fifo_drain2	186	0x100188c0
mv_fifo_elem_size	187	0x10017f00
mv_fifo_free	188	0x10018aa0
mv_fifo_freep	189	0x10018ae0
mv_fifo_freep2	190	0x10018950

Name	Ordinal	Address
mv_fifo_generic_peek	191	0x10019120
mv_fifo_generic_peek_at	192	0x10018fc0
mv_fifo_generic_read	193	0x10019160
mv_fifo_generic_write	194	0x10018e70
mv_fifo_grow	195	0x10018ce0
mv_fifo_grow2	196	0x10017f70
mv_fifo_peek	197	0x10018760
mv_fifo_peek_to_cb	198	0x100188a0
mv_fifo_read	199	0x10018500
mv_fifo_read_to_cb	200	0x100186c0
mv_fifo_realloc2	201	0x10018b70
mv_fifo_reset	202	0x10018b20
mv_fifo_reset2	203	0x10018930
mv_fifo_size	204	0x10018b40
mv_fifo_space	205	0x10018b50
mv_fifo_write	206	0x100180f0
mv_fifo_write_from_cb	207	0x100182a0
mv_file_map	208	0x100192e0
mv_file_unmap	209	0x10019570
mv_film_grain_params_alloc	210	0x10019b60
mv_film_grain_params_create_side_data	211	0x10019b90
mv_find_best_pix_fmt_of_2	212	0x10031f20
mv_find_info_tag	213	0x1002f8f0
mv_find_nearest_q_idx	214	0x10033340
mv_fopen_utf8	215	0x10019b50
mv_force_cpu_flags	216	0x1000f820
mv_fourcc_make_string	217	0x1008a3b0
mv_frame_alloc	218	0x1001ac40
mv_frame_apply_cropping	219	0x1001c490
mv_frame_clone	220	0x1001c050
mv_frame_copy	221	0x1001b8d0
mv_frame_copy_props	222	0x1001b550
mv_frame_free	223	0x1001adb0
mv_frame_get_buffer	224	0x1001adf0
mv_frame_get_plane_buffer	225	0x1001b570
mv_frame_get_side_data	226	0x1001b890
mv_frame_is_writable	227	0x1001b4b0
mv_frame_make_writable	228	0x1001c210
mv_frame_move_ref	229	0x1001b320
mv_frame_new_side_data	230	0x1001b7e0
mv_frame_new_side_data_from_buf	231	0x1001b750
mv_frame_ref	232	0x1001bc40
mv_frame_remove_side_data	233	0x1001c3e0
mv_frame_side_data_name	234	0x1001c470
mv_frame_unref	235	0x1001b300
mv_free	236	0x100265b0
mv_freep	237	0x100265c0
mv_gcd	238	0x10024570
mv_gcd_q	239	0x100337d0
mv_get_alt_sample_fmt	240	0x10039ed0
mv_get_bits_per_pixel	241	0x10031a80
mv_get_bytes_per_sample	242	0x1003a030
mv_get_channel_description	243	0x1000cf80
mv_get_channel_layout	244	0x1000c640
mv_get_channel_layout_channel_index	245	0x1000cd50
mv_get_channel_layout_nb_channels	246	0x1000cc80
mv_get_channel_layout_string	247	0x1000cbf0
mv_get_channel_name	248	0x1000cea0
mv_get_colorspace_name	249	0x1001ac20

Name	Ordinal	Address
mv_get_cpu_flags	250	0x1000f880
mv_get_default_channel_layout	251	0x1000cd10
mv_get_extended_channel_layout	252	0x1000c8f0
mv_get_known_color_name	253	0x1002ec40
mv_get_media_type_string	254	0x1008a240
mv_get_packed_sample_fmt	255	0x10039f10
mv_get_padded_bits_per_pixel	256	0x10031ad0
mv_get_picture_type_char	257	0x1008a260
mv_get_pix_fmt	258	0x10031960
mv_get_pix_fmt_loss	259	0x10031ef0
mv_get_pix_fmt_name	260	0x10031930
mv_get_pix_fmt_string	261	0x10031b80
mv_get_planar_sample_fmt	262	0x10039f50
mv_get_random_seed	263	0x10032510
mv_get_sample_fmt	264	0x10039d40
mv_get_sample_fmt_name	265	0x10039d20
mv_get_sample_fmt_string	266	0x10039f80
mv_get_standard_channel_layout	267	0x1000d150
mv_get_time_base_q	268	0x1008a470
mv_get_token	269	0x10006940
mv_gettime	270	0x1004b090
mv_gettime_relative	271	0x1004b0d0
mv_gettime_relative_is_monotonic	272	0x1004b140
mv_hash_alloc	273	0x1001c790
mv_hash_final	274	0x1001cb30
mv_hash_final_b64	275	0x1001ce80
mv_hash_final_bin	276	0x1001cbc0
mv_hash_final_hex	277	0x1001ce00
mv_hash_freep	278	0x1001d070
mv_hash_get_name	279	0x1001c770
mv_hash_get_size	280	0x1001c780
mv_hash_init	281	0x1001c870
mv_hash_names	282	0x1001c750
mv_hash_update	283	0x1001ca10
mv_hmac_alloc	284	0x1001d220
mv_hmac_calc	285	0x1001d720
mv_hmac_final	286	0x1001d5a0
mv_hmac_free	287	0x1001d3a0
mv_hmac_init	288	0x1001d3e0
mv_hmac_update	289	0x1001d590
mv_hwdevice_ctx_alloc	290	0x1001d920
mv_hwdevice_ctx_create	291	0x1001deb0
mv_hwdevice_ctx_create_derived	292	0x1001df50
mv_hwdevice_ctx_create_derived_opts	293	0x1001dee0
mv_hwdevice_ctx_init	294	0x1001d930
mv_hwdevice_find_type_by_name	295	0x1001d8a0
mv_hwdevice_get_hwframe_constraints	296	0x1001ddd0
mv_hwdevice_get_type_name	297	0x1001d8f0
mv_hwdevice_hwconfig_alloc	298	0x1001dda0
mv_hwdevice_iterate_types	299	0x1001d910
mv_hwframe_constraints_free	300	0x1001de70
mv_hwframe_ctx_alloc	301	0x1001d990
mv_hwframe_ctx_create_derived	302	0x1001e690
mv_hwframe_ctx_init	303	0x1001e450
mv_hwframe_get_buffer	304	0x1001e2f0
mv_hwframe_map	305	0x1001e0b0
mv_hwframe_transfer_data	306	0x1001db70
mv_hwframe_transfer_get_formats	307	0x1001db40
mv_i2int	308	0x10022490

Name	Ordinal	Address
mv_image_alloc	309	0x1001f200
mv_image_check_sar	310	0x1001f790
mv_image_check_size	311	0x1001f6a0
mv_image_check_size2	312	0x1001f550
mv_image_copy	313	0x1001faf0
mv_image_copy_plane	314	0x1001f9d0
mv_image_copy_plane_uc_from	315	0x1001f870
mv_image_copy_to_buffer	316	0x10020830
mv_image_copy_uc_from	317	0x1001ffd0
mv_image_fill_arrays	318	0x100204c0
mv_image_fill_black	319	0x10020b00
mv_image_fill_linesizes	320	0x1001eab0
mv_image_fill_max_pixsteps	321	0x1001e860
mv_image_fill_plane_sizes	322	0x1001ee90
mv_image_fill_pointers	323	0x1001efd0
mv_image_get_buffer_size	324	0x10020660
mv_image_get_linesize	325	0x1001e960
mv_int2i	326	0x10022460
mv_int_list_length_for_size	327	0x1008a280
mv_lfg_init	328	0x100a50ec
mv_lfg_init_from_data	329	0x100225e0
mv_log	330	0x10023a40
mv_log2	331	0x100224a0
mv_log2_16bit	332	0x100224b0
mv_log2_i	333	0x100212b0
mv_log_default_callback	334	0x10022ff0
mv_log_format_line	335	0x10023a30
mv_log_format_line2	336	0x10023730
mv_log_get_flags	337	0x10023bf0
mv_log_get_level	338	0x10023bc0
mv_log_once	339	0x10023ab0
mv_log_set_callback	340	0x10023c00
mv_log_set_flags	341	0x10023be0
mv_log_set_level	342	0x10023bd0
mv_lzo1x_decode	343	0x10023d50
mv_malloc	344	0x10026230
mv_malloc_array	345	0x100263a0
mv_mallocz	346	0x100265e0
mv_mallocz_array	347	0x10026400
mv_mastering_display_metadata_alloc	348	0x10024420
mv_mastering_display_metadata_create_side_data	349	0x10024440
mv_match_list	350	0x100075a0
mv_match_name	351	0x10007100
mv_max_alloc	352	0x10026220
mv_md5_alloc	353	0x10025c70
mv_md5_final	354	0x10025ed0
mv_md5_init	355	0x10025c90
mv_md5_size	356	0x100b3b48
mv_md5_sum	357	0x10025fe0
mv_md5_update	358	0x10025cc0
mv_memcpy_backptr	359	0x10026d10
mv_memdup	360	0x10026980
mv_mod_i	361	0x100218a0
mv_mul_i	362	0x10021340
mv_mul_q	363	0x10032da0
mv_murmur3_alloc	364	0x100274a0
mv_murmur3_final	365	0x10027ce0
mv_murmur3_init	366	0x100275b0
mv_murmur3_init_seeded	367	0x100274c0

Name	Ordinal	Address
mv_murmur3_update	368	0x10027690
mv_nearer_q	369	0x10033180
mv_opt_child_class_iterate	370	0x1002d880
mv_opt_child_next	371	0x1002d860
mv_opt_copy	372	0x1002d910
mv_opt_eval_double	373	0x1002cb00
mv_opt_eval_flags	374	0x1002ca00
mv_opt_eval_float	375	0x1002cac0
mv_opt_eval_int	376	0x1002ca40
mv_opt_eval_int64	377	0x1002ca80
mv_opt_eval_q	378	0x1002cb40
mv_opt_find	379	0x1002c350
mv_opt_find2	380	0x1002c140
mv_opt_flag_is_set	381	0x1002d7b0
mv_opt_free	382	0x1002c0b0
mv_opt_freep_ranges	383	0x1002dc40
mv_opt_get	384	0x1002ad50
mv_opt_get_channel_layout	385	0x1002b9a0
mv_opt_get_chlayout	386	0x1002ba30
mv_opt_get_dict_val	387	0x1002bac0
mv_opt_get_double	388	0x1002b3e0
mv_opt_get_image_size	389	0x1002b680
mv_opt_get_int	390	0x1002b270
mv_opt_get_key_value	391	0x1002bf30
mv_opt_get_pixel_fmt	392	0x1002b8a0
mv_opt_get_q	393	0x1002b4f0
mv_opt_get_sample_fmt	394	0x1002b920
mv_opt_get_video_rate	395	0x1002b710
mv_opt_is_set_to_default	396	0x1002dce0
mv_opt_is_set_to_default_by_name	397	0x1002e260
mv_opt_next	398	0x10029c40
mv_opt_ptr	399	0x1002d8a0
mv_opt_query_ranges	400	0x1002dbe0
mv_opt_query_ranges_default	401	0x10028ed0
mv_opt_serialize	402	0x1002e2b0
mv_opt_set	403	0x1002cb80
mv_opt_set_bin	404	0x1008a930
mv_opt_set_channel_layout	405	0x1002ac10
mv_opt_set_chlayout	406	0x1002ad00
mv_opt_set_defaults	407	0x1002bf10
mv_opt_set_defaults2	408	0x1002bb90
mv_opt_set_dict	409	0x1002d780
mv_opt_set_dict2	410	0x1002d660
mv_opt_set_dict_val	411	0x1002ac90
mv_opt_set_double	412	0x10029eb0
mv_opt_set_from_string	413	0x1002d400
mv_opt_set_image_size	414	0x1002a600
mv_opt_set_int	415	0x10029c90
mv_opt_set_pixel_fmt	416	0x1002a9f0
mv_opt_set_q	417	0x1002a1a0
mv_opt_set_sample_fmt	418	0x1002ab00
mv_opt_set_video_rate	419	0x1002a6c0
mv_opt_show2	420	0x1002bb20
mv_parse_color	421	0x1002e900
mv_parse_cpu_caps	422	0x1000f8b0
mv_parse_ratio	423	0x1002e5d0
mv_parse_time	424	0x1002f110
mv_parse_video_rate	425	0x1002e7a0
mv_parse_video_size	426	0x1002e6e0

Name	Ordinal	Address
mv_pix_fmt_count_planes	427	0x10031d50
mv_pix_fmt_desc_get	428	0x10031c70
mv_pix_fmt_desc_get_id	429	0x10031ce0
mv_pix_fmt_desc_next	430	0x10031ca0
mv_pix_fmt_get_chroma_sub_sample	431	0x10031d10
mv_pix_fmt_swap_endianness	432	0x10031e00
mv_pixelutils_get_sad_fn	433	0x100324e0
mv_q2intfloat	434	0x10033570
mv_rc4_alloc	435	0x100338c0
mv_rc4_crypt	436	0x100339c0
mv_rc4_init	437	0x100338e0
mv_read_image_line	438	0x10030ea0
mv_read_image_line2	439	0x10030750
mv_realloc	440	0x10026280
mv_realloc_array	441	0x100264f0
mv_realloc_f	442	0x100262c0
mv_reallocp	443	0x10026320
mv_reallocp_array	444	0x10026530
mv_reduce	445	0x10032890
mv_rescale	446	0x10024c40
mv_rescale_delta	447	0x10024f60
mv_rescale_q	448	0x10024cc0
mv_rescale_q_rnd	449	0x10024c90
mv_rescale_rnd	450	0x10024700
mv_ripemd_alloc	451	0x10039950
mv_ripemd_final	452	0x10039bc0
mv_ripemd_init	453	0x100a5198
mv_ripemd_size	454	0x100bc2e4
mv_ripemd_update	455	0x10039970
mv_sample_fmt_is_planar	456	0x1003a050
mv_samples_alloc	457	0x1003a320
mv_samples_alloc_array_and_samples	458	0x1003a4f0
mv_samples_copy	459	0x1003a750
mv_samples_fill_arrays	460	0x1003a1b0
mv_samples_get_buffer_size	461	0x1003a070
mv_samples_set_silence	462	0x1003a930
mv_set_options_string	463	0x1002d230
mv_sha512_alloc	464	0x10049740
mv_sha512_final	465	0x100499a0
mv_sha512_init	466	0x100a53bc
mv_sha512_size	467	0x100bc42c
mv_sha512_update	468	0x10049760
mv_sha_alloc	469	0x1003e680
mv_sha_final	470	0x1003e8f0
mv_sha_init	471	0x100a52c0
mv_sha_size	472	0x100bc424
mv_sha_update	473	0x1003e6a0
mv_shr_i	474	0x10021760
mv_size_mult	475	0x10027480
mv_small_strptime	476	0x1002ec70
mv_spherical_alloc	477	0x1004a600
mv_spherical_from_name	478	0x1004a760
mv_spherical_projection_name	479	0x1004a740
mv_spherical_tile_bounds	480	0x1004a630
mv_sscanf	481	0x10002f80
mv_stereo3d_alloc	482	0x1004a7b0
mv_stereo3d_create_side_data	483	0x1004a7d0
mv_stereo3d_from_name	484	0x1004a840
mv_stereo3d_type_name	485	0x1004a820

Name	Ordinal	Address
mv_strcasecmp	486	0x10006b30
mv_strdup	487	0x100267c0
mv_strerror	488	0x10013b30
mv_strireplace	489	0x10006bf0
mv_stristart	490	0x10006580
mv_stristr	491	0x100065f0
mv_strlcat	492	0x10006750
mv_strlcatf	493	0x100067f0
mv_strlcpy	494	0x100066e0
mv_strncasecmp	495	0x10006b80
mv_strndup	496	0x10026890
mv_strnstr	497	0x10006660
mv_strstart	498	0x10006530
mv_strtod	499	0x100150e0
mv_strtok	500	0x10006aa0
mv_sub_i	501	0x100211e0
mv_sub_q	502	0x10032ef0
mv_tea_alloc	503	0x1004a940
mv_tea_crypt	504	0x1004a990
mv_tea_init	505	0x1004a960
mv_tea_size	506	0x100bc5a0
mv_tempfile	507	0x100195a0
mv_thread_message_flush	508	0x1004b020
mv_thread_message_queue_alloc	509	0x1004abe0
mv_thread_message_queue_free	510	0x1004acb0
mv_thread_message_queue_nb_elems	511	0x1004ad60
mv_thread_message_queue_recv	512	0x1004ae90
mv_thread_message_queue_send	513	0x1004adb0
mv_thread_message_queue_set_err_recv	514	0x1004afd0
mv_thread_message_queue_set_err_send	515	0x1004af80
mv_thread_message_queue_set_free_func	516	0x1004aca0
mv_timecode_adjust_ntsc_framenum2	517	0x1004b210
mv_timecode_check_frame_rate	518	0x1004bda0
mv_timecode_get_smpte	519	0x1004b560
mv_timecode_get_smpte_from_framenum	520	0x1004b2b0
mv_timecode_init	521	0x1004be10
mv_timecode_init_from_components	522	0x1004bf30
mv_timecode_init_from_string	523	0x1004c160
mv_timecode_make_mpeg_tc_string	524	0x1004bd30
mv_timecode_make_smpte_tc_string	525	0x1004bc00
mv_timecode_make_smpte_tc_string2	526	0x1004ba00
mv_timecode_make_string	527	0x1004b750
mv_timegm	528	0x1002f030
mv_tree_destroy	529	0x1004cdd0
mv_tree_enumerate	530	0x1004cfb0
mv_tree_find	531	0x1004c440
mv_tree_insert	532	0x1004c500
mv_tree_node_alloc	533	0x1004c420
mv_tree_node_size	534	0x100bc6c0
mv_twofish_alloc	535	0x1004d570
mv_twofish_crypt	536	0x1004d590
mv_twofish_init	537	0x100a5843
mv_twofish_size	538	0x100bc6e0
mv_tx_init	539	0x100a6a4f
mv_tx_uninit	540	0x100a6137
mv_usleep	541	0x1004b150
mv_utf8_decode	542	0x10007270
mv_util_ffversion	543	0x100c27e0
mv_uuid_parse	544	0x1008a5f0

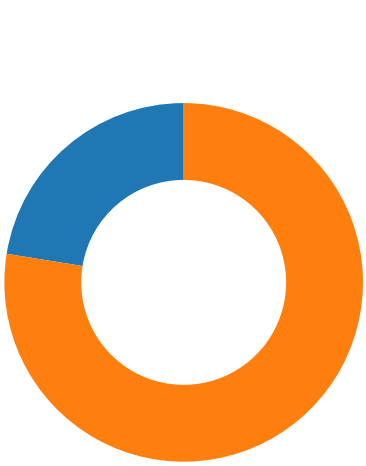
Name	Ordinal	Address
mv_uuid_parse_range	545	0x1008a4d0
mv_uuid_unparse	546	0x1008a640
mv_uuid_urn_parse	547	0x1008a8c0
mv_vbprintf	548	0x10008b70
mv_version_info	549	0x1008a920
mv_video_enc_params_alloc	550	0x1008a960
mv_video_enc_params_create_side_data	551	0x1008a9e0
mv_vk_frame_alloc	552	0x1001e850
mv_vkfmt_from_pixfmt	553	0x1001e840
mv_vlog	554	0x10023b30
mv_write_image_line	555	0x100316f0
mv_write_image_line2	556	0x10031350
mv_xtea_alloc	557	0x1008dc40
mv_xtea_crypt	558	0x1008dcb0
mv_xtea_init	559	0x1008dc60
mv_xtea_le_crypt	560	0x1008ddf0
mv_xtea_le_init	561	0x1008dc90
mvpriv_alloc_fixed_dsp	562	0x10019fa0
mvpriv_cga_font	563	0x100c4220
mvpriv_dict_set_timestamp	564	0x10012370
mvpriv_float_dsp_alloc	565	0x100a4ff0
mvpriv_fopen_utf8	566	0x10019a90
mvpriv_get_gamma_from_trc	567	0x1000f7d0
mvpriv_get_trc_function_from_trc	568	0x1000f800
mvpriv_init_lls	569	0x100a5164
mvpriv_open	570	0x100195e0
mvpriv_report_missing_feature	571	0x10023cc0
mvpriv_request_sample	572	0x10023c10
mvpriv_scalarproduct_float_c	573	0x1001a2e0
mvpriv_set_systematic_pal2	574	0x1001f0d0
mvpriv_slicethread_create	575	0x1004a330
mvpriv_slicethread_execute	576	0x1004a030
mvpriv_slicethread_free	577	0x1004a200
mvpriv_solve_lls	578	0x10022750
mvpriv_tempfile	579	0x10019970
mvpriv_vga16_font	580	0x100c3220
mvutil_configuration	581	0x1008a940
mvutil_license	582	0x1008a950
next	583	0x1002a4a0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 18:12:48.615066051 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:48.615134001 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:48.615257025 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:48.623416901 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:48.623470068 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:48.981170893 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:48.981367111 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:48.981406927 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:48.981465101 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.200453997 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.200494051 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:49.201351881 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:49.201536894 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.203943968 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.244297981 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:49.317714930 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:49.317821980 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:49.317917109 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.317944050 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.321155071 CEST	49719	443	192.168.2.3	147.154.26.35
May 30, 2023 18:12:49.321206093 CEST	443	49719	147.154.26.35	192.168.2.3
May 30, 2023 18:12:49.604969025 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:49.675036907 CEST	2222	49722	109.50.149.241	192.168.2.3
May 30, 2023 18:12:49.675148010 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:49.676702976 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:49.757062912 CEST	2222	49722	109.50.149.241	192.168.2.3
May 30, 2023 18:12:49.757194996 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:50.453862906 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:50.523997068 CEST	2222	49722	109.50.149.241	192.168.2.3
May 30, 2023 18:12:50.524228096 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:50.528815985 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:12:50.679574013 CEST	2222	49722	109.50.149.241	192.168.2.3
May 30, 2023 18:12:50.679675102 CEST	49722	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.350507975 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.418210030 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.418342113 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.419131994 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.486851931 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.486948013 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.487500906 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.490263939 CEST	49724	2222	192.168.2.3	109.50.149.241

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 18:13:08.490432978 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.557344913 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.557421923 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.557593107 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.557625055 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.557677031 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.557677984 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.557691097 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.557756901 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.557756901 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.624886036 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.624960899 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.625077963 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.625150919 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.625241041 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.625268936 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.625366926 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.692204952 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692347050 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692459106 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692485094 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692517996 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692548990 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.692611933 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.692646027 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.692707062 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692768097 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.692864895 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.692975998 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.693027973 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.693073034 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.693140030 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.693159103 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.693180084 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.693181992 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.693250895 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.693296909 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.693392992 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.759692907 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.759735107 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.759804964 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.759826899 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.759838104 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.759891987 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.759922028 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760044098 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760128975 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760217905 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.760438919 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760596037 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760656118 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760700941 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.760727882 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.760786057 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760905027 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760929108 CEST	2222	49724	109.50.149.241	192.168.2.3
May 30, 2023 18:13:08.760993958 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.761010885 CEST	49724	2222	192.168.2.3	109.50.149.241
May 30, 2023 18:13:08.761044979 CEST	2222	49724	109.50.149.241	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 30, 2023 18:12:48.579852104 CEST	192.168.2.3	8.8.8.8	0x940a	Standard query (0)	oracle.com	A (IP address)	IN (0x0001)	false
May 30, 2023 18:12:49.325193882 CEST	192.168.2.3	8.8.8.8	0x95c0	Standard query (0)	www.oracle.com	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.544575930 CEST	192.168.2.3	8.8.8.8	0x966c	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:21.164458990 CEST	192.168.2.3	8.8.8.8	0xc001	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 30, 2023 18:12:48.608320951 CEST	8.8.8.8	192.168.2.3	0x940a	No error (0)	oracle.com		147.154.26.35	A (IP address)	IN (0x0001)	false
May 30, 2023 18:12:49.360934019 CEST	8.8.8.8	192.168.2.3	0x95c0	No error (0)	www.oracle.com	ds-www.oracle.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		54.161.105.65	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		34.225.127.72	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:20.568216085 CEST	8.8.8.8	192.168.2.3	0x966c	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:21.187855005 CEST	8.8.8.8	192.168.2.3	0xc001	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)	false
May 30, 2023 18:13:21.187855005 CEST	8.8.8.8	192.168.2.3	0xc001	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)	false
May 30, 2023 18:13:21.187855005 CEST	8.8.8.8	192.168.2.3	0xc001	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- oracle.com
- yahoo.com
- www.yahoo.com

Statistics

Behavior

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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **7380**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:09:35
Start date:	30/05/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\main2.dll"
Imagebase:	0x8a0000
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: **7388**, Parent PID: **7380**

General

Target ID:	1
Start time:	18:09:35
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **7416**, Parent PID: **7380**

General

Target ID:	2
Start time:	18:09:35
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\main2.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: **7424**, Parent PID: **7380**

General

Target ID:	3
Start time:	18:09:35
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\main2.dll,mv_add_i
Imagebase:	0x1120000
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: **7436**, Parent PID: **7416**

General

Target ID:	4
Start time:	18:09:35
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",#1

Imagebase:	0x1120000
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: **7536**, Parent PID: **7424**

General

Target ID:	8
Start time:	18:09:36
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7424 -s 652
Imagebase:	0xfd0000
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	6C7A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CEB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CEB.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d1db9c8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d1db9c8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CEB.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CEB.tmp.xml	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D19.tmp.csv	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F3E.tmp.txt	success or wait	1	6C79497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 51 fd 76 64 fd 05 12 00 00 00 00 00	MDMP Qvd	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.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 00 1d 00 00 4f fd 76 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBGenuineIntelWTOvd0 =Pacific Standard TimePacific Daylight T ime	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 10 11 02 10 60 3d 6c 03 00 00 00 00 fd 04 01 00 00 00 12 01 1c fd 09 01 fd 11 02 10 23 00 00 00 46 02 01 00 fd fd 09 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++`=l#F+	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	1620	168	04 1d 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 11 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 7e 21 00 00	~!	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	10722	20	0b 00 00 00 00 20 29 03 00 00 00 00 fd 04 00 00 fd 2a 00 00	)*	success or wait	11	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	10902	1176	00 00 00 04 fd fd fd 00 00 12 01 fd 7b fd 77 48 17 6b 03 00 00 00 00 00 00 6b 03 fd 79 fd 77 00 00 00 00 00 00 00 00 04 00 00 00 00 10 fd 74 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 fd 7b fd 77 fd fd fd fd 01 00 00 00 00 00 7d 7f 00 00 00 00 30 07 7d 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 03 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{wHkkywt{w}0}(Pm `fwPSwB	success or wait	10	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	26654	980	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 fd fd 1d 03 fd fd 1d 03 fd fd fd fd 40 cc 77 40 cc 77 08 06 6c 03 00 fd 29 03 00 fd 29 03 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd 29 03 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 06 6c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 6b 03 00 00 00 00 00 00 00 00 fd 07 6c 03 00 20 29 03 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 06 6c 03 00 00 00 00 fd fd fd fd fd fd fd 54 22 29 03 54 22 29 03 40 06 6c 03 40 06 6c 03 00 00 00 00 fd fd fd fd 08 06 6c 03 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@wl))PP)lkl)lT")T")@l@ll	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.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 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 fd fd 09 01 fd fd fd 77 23 00 00 00 12 02 00 00 20 fd 09 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w# +	success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	1840	48	14 1d 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 29 03 00 00 00 00 2c fd 1d 03 00 00 00 00 fd 03 00 00 1e 68 00 00 fd 02 00 00 16 27 00 00	),h'	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 05 03 00 00 00 00 2c 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 07 2d 04 00 00 00 00 00 00 00 00 00 00 00 00 00 25 fd 1a 00 00 00 00 00 1b 50 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6b 05 00 00 00 00	s0Us@d!BB?#@AZb,-%P@k	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.tmp.dmp	27634	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB7.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 76 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8Tv	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7424</Pid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1794</Uptime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 35 00 34 00 32 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>124542976</PeakVirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 35 00 33 00 34 00 37 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>124534784</VirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 36 00 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>2360</PageFaultCount>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 31 00 31 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>7901184</PeakWorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 31 00 31 00 38 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>7901184</WorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 33 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>180384</QuotaPeakPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 31 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>180184</QuotaPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24160</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23888</QuotaNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 31 00 31 00 39 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>6311936</PagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 32 00 30 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>63201280</PeakPagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 31 00 31 00 39 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>6311936</PrivateUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 33 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7380</Pid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2018</Uptime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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 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>889</PageFaultCount>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 33 00 31 00 37 00 34 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>3231744</PeakWorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 32 00 39 00 33 00 34 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>3129344</WorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4254	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>638976</PagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4342	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 32 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>1892352</PeakPagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4434	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4438	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4448	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>638976</PrivateUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4518	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4522	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4530	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4576	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4580	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4586	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4628	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4632	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4636	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4674	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4722	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4760	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4764	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4768	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	8	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	16	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	4838	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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 6f 00 74 00 75 00 79 00 69 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>otuyin, Inc.</SystemManufacturer>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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 6f 00 74 00 75 00 79 00 69 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>otuyin7,1</SystemProductName>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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 34 00 33 00 31 00 37 00 35 00 35 00 39 00 30 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>1643175590</OSInstallDate>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7006	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	6	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7464	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 31 00 3a 00 30 00 39 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T01:09:37Z">	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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 38 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 34 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="384" PID="7424" UptimeMS="171" TimeSinceCreationMS="171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 37 00 65 00 35 00 66 00 39 00 37 00 35 00 2d 00 61 00 65 00 36 00 35 00 2d 00 34 00 65 00 62 00 65 00 2d 00 38 00 65 00 61 00 34 00 2d 00 63 00 30 00 35 00 39 00 32 00 61 00 31 00 62 00 64 00 30 00 39 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>17e5f975-ae65-4ebe-8ea4-c0592a1bd097</Guid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 31 00 3a 00 30 00 39 00 3a 00 33 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T01:09:37Z</CreationTime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAC.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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CEB.tmp.xml	0	4628	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d1db9c8\Report.wer	0	2	fd fd		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d1db9c8\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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d1db9c8\Report.wer	11326	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 39 00 38 00 34 00 30 00 37 00 33 00 37 00 37 00 33 00	MetadataHash=-984073773	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7B36BF	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7943D1	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 C3 11 02 10 02 00 00 00 01 00 00 00 AE 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 C3 11 02 10 02 00 00 00 01 00 00 00 AA 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C7B1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **7528**, Parent PID: **7436**

General

Target ID:	9
Start time:	18:09:36
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7436 -s 660
Imagebase:	0xfd0000
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	6C7A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CFB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CFB.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d05b9a9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d05b9a9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CFB.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CFB.tmp.xml	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.csv	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F0E.tmp.txt	success or wait	1	6C79497A	unknown

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 51 fd 76 64 fd 05 12 00 00 00 00 00	MDMP Qvd	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 0c 1d 00 00 4f fd 76 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBGenuineIntelWTOvd0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 10 11 02 10 fd fd fd 00 00 00 00 00 fd 04 01 00 00 00 12 01 fd fd fd 00 fd 11 02 10 23 00 00 00 46 02 01 00 58 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++#FX+	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	1620	168	10 1d 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 11 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 7e 21 00 00	~!	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	10722	20	0b 00 00 00 fd fd fd 00 00 00 00 00 24 17 00 00 fd 2a 00 00	$*	success or wait	11	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	10902	5924	fd fd fd 77 fd 1a fd 76 fd fd fd fd 10 fd fd 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 30 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv$0	success or wait	10	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	26974	2340	fd fd fd 77 fd 4c 77 58 02 00 00 fd fd fd fd 10 00 00 00 70 fd 78 04 3c fd 78 04 fd fd fd fd 40 cc 77 40 cc 77 fd 04 fd 00 00 fd fd 00 00 fd fd 00 00 00 00 00 58 02 00 00 fd fd fd fd 58 02 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 10 fd fd 00 00 00 00 00 00 00 00 00 50 06 fd 00 00 30 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 fd 00 00 00 00 00 fd fd fd fd fd fd fd 54 32 fd 00 54 32 fd 00 fd 04 fd 00 fd 04 fd 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwXpx<x@w@wXXP0T2T2	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.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 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 70 fd fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++pw#+	success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	1840	48	20 1d 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 78 04 00 00 00 00 24 09 00 00 5e 69 00 00 fd 02 00 00 16 27 00 00	x$^i'	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 05 03 00 00 00 00 31 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 07 2d 04 00 00 00 00 00 00 00 00 00 00 00 00 00 af 1a 00 00 00 00 00 62 4f 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6b 05 00 00 00 00	s0Us@d!BB?#@AZb1-bO@k	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.tmp.dmp	29314	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AC6.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 74 7d 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)T8TPt}	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 34 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7436</Pid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1715</Uptime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 35 00 34 00 32 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>124542976</PeakVirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 35 00 33 00 34 00 37 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>124534784</VirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 36 00 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>2361</PageFaultCount>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 37 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7917568</PeakWorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 37 00 35 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7917568</WorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 33 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>180384</QuotaPeakPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 31 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>180184</QuotaPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24160</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23888</QuotaNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 38 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6287360</PagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 39 00 35 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6295552</PeakPagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 38 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6287360</PrivateUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 34 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7416</Pid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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 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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 35 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1853</Uptime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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 30 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>1108</PageFaultCount>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3686400</PeakWorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 34 00 31 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3674112</WorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3878	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 30 00 31 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3420160</PagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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 33 00 38 00 39 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3538944</PeakPagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 30 00 31 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3420160</PrivateUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5440	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5444	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5446	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5486	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5490	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5492	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5530	4	0d 00 0a 00		success or wait	6	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5534	2	09 00		success or wait	12	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	5538	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6092	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6096	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6098	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6138	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6142	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6144	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6182	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6186	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6190	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6284	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6288	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6292	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 6f 00 74 00 75 00 79 00 69 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>otuyin, Inc.</SystemManufacturer>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6398	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6402	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6406	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 6f 00 74 00 75 00 79 00 69 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>otuyin7,1</SystemProductName>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6502	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6506	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6510	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6630	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6634	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6638	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 33 00 31 00 37 00 35 00 35 00 39 00 30 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>1643175590</OSInstallDate>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6720	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6724	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6728	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6830	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6834	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6838	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6912	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6952	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6956	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6958	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6992	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	6996	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7000	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7096	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7100	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7102	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7144	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7168	4	0d 00 0a 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7172	2	09 00		success or wait	6	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7176	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7420	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7424	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7426	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7452	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7456	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7458	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 31 00 3a 00 30 00 39 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T01:09:37Z">	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7558	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7562	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7566	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 34 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 34 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 34 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="385" PID="7436" UptimeMS="140" TimeSinceCreationMS="140" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7824	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7828	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7832	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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7852	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7856	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7858	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7896	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7900	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7902	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	7948	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 65 00 63 00 63 00 63 00 64 00 34 00 36 00 2d 00 66 00 37 00 33 00 62 00 2d 00 34 00 32 00 32 00 66 00 2d 00 39 00 30 00 33 00 37 00 2d 00 37 00 38 00 61 00 65 00 31 00 34 00 31 00 35 00 32 00 66 00 30 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5ecccd46-f73b-422f-9037-78ae14152f03</Guid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8054	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 31 00 3a 00 30 00 39 00 3a 00 33 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T01:09:37Z</CreationTime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8158	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CBB.tmp.WERInternalMetadata.xml	8202	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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CFB.tmp.xml	0	4628	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d05b9a9\Report.wer	0	2	fd fd		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d05b9a9\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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c55aaf39bde8f13d445c6aad2c0a878a5c24_82810a17_1d05b9a9\Report.wer	11324	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 37 00 33 00 33 00 39 00 39 00 39 00 38 00 38 00 31 00	MetadataHash=1733999881	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6C7B1FB2	RegCreateKeyExW
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6C7943D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 C3 11 02 10 02 00 00 00 01 00 00 00 AE 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C7B1FE8	RegSetValueExW
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7943D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C7943D1	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6C7943D1	unknown

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

Analysis Process: rundll32.exe PID: **7644**, Parent PID: **7380**

General

Target ID:	10
Start time:	18:09:38
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\main2.dll,mv_add_q
Imagebase:	0x1120000
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: **7672**, Parent PID: **7380**

General

Target ID:	11
Start time:	18:09:41
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\main2.dll,mv_add_stable
Imagebase:	0x1120000
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: **7708**, Parent PID: **7672**

General

Target ID:	13
Start time:	18:09:42
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7672 -s 656
Imagebase:	0xfd0000
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	6C7A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e71ba64	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e71ba64\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C79497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp.xml	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19E.tmp.csv	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB299.tmp.txt	success or wait	1	6C79497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 56 fd 76 64 fd 05 12 00 00 00 00 00	MDMP Vvd	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.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 1d 00 00 55 fd 76 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBGenuineIntelWTUvd0 =Pacific Standard TimePacific Daylight T ime	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 2b fd 08 10 23 00 00 00 46 02 01 00 fd fd 75 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+++#Fu+	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	1620	168	fd 1d 00 00 00 00 00 00 fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 2b fd 08 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 7e 21 00 00	+~!	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	10722	20	0b 00 00 00 00 06 fd 00 00 00 00 00 04 00 00 00 fd 2a 00 00	*	success or wait	11	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	10902	4	68 fd fd 00	h	success or wait	10	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	27722	256	00 00 00 fd 89 fd 31 89 4b 54 24 10 fd 5c 24 0c fd fd 74 07 fd 43 fd 00 fd cb 44 24 04 fd fd 74 07 fd 83 fd 00 fd cb 44 24 50 fd 89 30 fd 78 04 fd fd 2c fd fd 5b 5e 5f 5d cd 76 00 0f fd c3 fd 1f fd 44 24 0c 75 54 39 fd 0f fd 04 01 00 00 31 fd 39 74 24 08 0f fd fd 00 00 00 fd 89 fd 8d fd 26 00 00 00 00 fd 76 00 fd fd 75 0b fd 01 00 00 00 31 fd fd fd 89 fd 31 fd fd fd fd 4b 44 24 08 fd 6c 24 0c fd fd fd 44 24 08 fd 49 fd fd fd fd fd 00 00 00 00 fd 54 24 0c fd 20 00 00 00 29 09 49 fd fd fd fd fd fd fd fd 09 fd fd fd c9 fd fd 44 24 14 fd fd fd 6c 24 08 fd fd fd fd fd fd fd fd fd 09 4b 54 24 08 fd 49 49 fd fd fd fd 54 24 1c fd fd fd 74 24 14 fd c9 fd fd fd fd	1T$\$tDtDP0x, [^_]vD$uT919t$& vu11DIDIT)DITTt$	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 75 00 fd fd fd 77 23 00 00 00 16 02 00 00 60 fd 75 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++uw#`u+	success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	1840	48	00 1e 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 6c 04 00 00 fd 67 00 00 fd 02 00 00 16 27 00 00	Plg'	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.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	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.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 60 fd 02 00 00 00 00 00 fd 05 03 00 00 00 00 0d 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 07 2d 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 67 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 7c 05 00 00 00 00	s0Us@d!BB?#@AZb`-g@|	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.tmp.dmp	27978	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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFA6.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 20 78 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8T x	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 36 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7672</Pid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1178	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>981</Uptime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1430	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 35 00 34 00 32 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>124542976</PeakVirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1528	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 34 00 35 00 33 00 34 00 37 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>124534784</VirtualSize>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 36 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>2361</PageFaultCount>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 33 00 34 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>7913472</PeakWorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 33 00 34 00 37 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>7913472</WorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 33 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>180384</QuotaPeakPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 31 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>180184</QuotaPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 30 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>24000</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 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>23728</QuotaNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 38 00 33 00 32 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6283264</PagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 39 00 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6291456</PeakPagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 38 00 33 00 32 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6283264</PrivateUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 37 00 33 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7380</Pid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2830	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	2914	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 33 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7342</Uptime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3070	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3286	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 31 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17121280</PeakVirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3386	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 39 00 30 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13090816</VirtualSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3470	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 39 00 35 00 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>953</PageFaultCount>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3556	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 33 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3235840</PeakWorkingSetSize>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3666	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 32 00 39 00 33 00 34 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>3129344</WorkingSetSize>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3760	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>77976</QuotaPeakPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3886	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3986	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	3996	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4132	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4136</QuotaNonPagedPoolUsage>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4252	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>638976</PagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4340	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 32 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>1892352</PeakPagefileUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4446	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>638976</PrivateUsage>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5450	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5496	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	5542	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6102	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6148	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6194	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6296	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6f 00 74 00 75 00 79 00 69 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>otuyin, Inc.</SystemManufacturer>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6406	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6410	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6f 00 74 00 75 00 79 00 69 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>otuyin7,1</SystemProductName>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6514	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6642	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 33 00 31 00 37 00 35 00 35 00 39 00 30 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>1643175590</OSInstallDate>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6732	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6842	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6916	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6962	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7004	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7106	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7148	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7180	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7430	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7462	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 31 00 3a 00 30 00 39 00 3a 00 34 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T01:09:42Z">	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7570	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 36 00 37 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 31 00 34 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 34 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="394" PID="7672" UptimeMS="140" TimeSinceCreationMS="140" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7836	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7862	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7906	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 33 00 66 00 37 00 30 00 30 00 62 00 61 00 2d 00 37 00 64 00 63 00 38 00 2d 00 34 00 66 00 31 00 30 00 2d 00 39 00 38 00 33 00 33 00 2d 00 39 00 37 00 31 00 32 00 35 00 38 00 31 00 61 00 63 00 35 00 32 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e3f700ba-7dc8-4f10-9833-9712581ac523</Guid>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8058	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 31 00 3a 00 30 00 39 00 3a 00 34 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T01:09:42Z</CreationTime>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8162	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB13D.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp.xml	0	4628	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e71ba64\Report.wer	0	2	fd fd		success or wait	1	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e71ba64\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	6C79497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c56e6db63eb6a43e45028e0a8fb2e35516856f4_82810a17_1e71ba64\Report.wer	11326	40	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 32 00 34 00 38 00 36 00 34 00 34 00 35 00	MetadataHash=2486445	success or wait	1	6C79497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7B36BF	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7B36BF	unknown
\REGISTRY\A\{a11be96c-3191-167b-9123-1d6c5b7cffd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7943D1	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 C3 11 02 10 02 00 00 00 01 00 00 00 AA 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	94 00 00 C0 00 00 00 00 00 00 00 00 2B F0 08 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C7B1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **7768**, Parent PID: **7380**

General	
Target ID:	14
Start time:	18:09:44
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",mv_add_i
Imagebase:	0x1120000
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: **7796**, Parent PID: **7380**

General	
Target ID:	15
Start time:	18:09:44
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",mv_add_q
Imagebase:	0x1120000
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: **7808**, Parent PID: **7380**

General	
Target ID:	16
Start time:	18:09:44
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",mv_add_stable
Imagebase:	0x1120000
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: **7816**, Parent PID: **7380**

General	
Target ID:	17
Start time:	18:09:45
Start date:	30/05/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",next
Imagebase:	0x1120000
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: 00000011.00000002.407663354.00000000004FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000011.00000002.409110977.0000000000E30000.00000004.00000020.00020000.00000000.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: 7836, Parent PID: 7380

General

Target ID:	18
Start time:	18:09:45
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",mvutil_license
Imagebase:	0x1120000
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: 7844, Parent PID: 7380

General

Target ID:	19
Start time:	18:09:45
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\main2.dll",mvutil_configuration
Imagebase:	0x1120000
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: 7916, Parent PID: 7768

General

Target ID:	22
Start time:	18:09:45
Start date:	30/05/2023

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7768 -s 656
Imagebase:	0xfd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **7932**, Parent PID: **7808**

General	
Target ID:	23
Start time:	18:09:46
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7808 -s 660
Imagebase:	0xfd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: **8032**, Parent PID: **7816**

General	
Target ID:	24
Start time:	18:09:49
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0xc80000
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: **7132**, Parent PID: **8032**

General	
Target ID:	29
Start time:	18:12:50
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0x1070000
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: **7136**, Parent PID: **7132**

General

Target ID:	30
Start time:	18:12:50
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: **3124**, Parent PID: **8032**

General

Target ID:	31
Start time:	18:12:50
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0x70000
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: **7880**, Parent PID: **3124**

General

Target ID:	32
Start time:	18:12:50
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msiexec.exe PID: **3780**, Parent PID: **580**

General

Target ID:	34

Start time:	18:12:51
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7f1280000
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