ID: 880144
Sample Name: qbot1.dll
Cookbook: default.jbs
Time: 21:22:57
Date: 01/06/2023
Version: 37.1.0 Beryl

Table of Contents

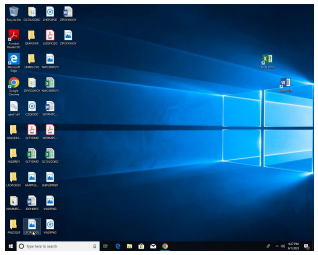
Windows Analysis Report

qbot1.dll

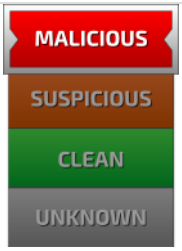
Overview

General Information

Sample Name:	qbot1.dll
Analysis ID:	880144
MD5:	682b7633158d…
SHA1:	1f409c817fdf4d..
SHA256:	83380409b59c…
Infos:	



Detection



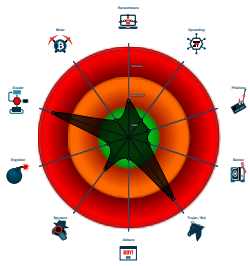
Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Multi AV Scanner detection for subm…
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- 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: 5568 cmdline: loaddll32.exe "C:\Users\user\Desktop\qbot1.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 6356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6348 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6268 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6644 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6268 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6336 cmdline: rundll32.exe C:\Users\user\Desktop\qbot1.dll,m?0API@ScScript@@IAE@AAVEngine@1@H@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6648 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6336 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5044 cmdline: rundll32.exe C:\Users\user\Desktop\qbot1.dll,m?0BinaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@1@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7044 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5044 -s 672 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5772 cmdline: rundll32.exe C:\Users\user\Desktop\qbot1.dll,m?0BreakpointInfo@ScScript@@QAE@ABV01@@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7072 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5772 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7156 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",m?0API@ScScript@@IAE@AAVEngine@1@H@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6612 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7156 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5444 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",m?0BinaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@1@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6868 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5444 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5428 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",m?0BreakpointInfo@ScScript@@QAE@ABV01@@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6504 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5428 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7020 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7148 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
      - ipconfig.exe (PID: 2244 cmdline: ipconfig /all MD5: B0C7423D02A007461C850CD0DFE09318)
        - conhost.exe (PID: 4332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 5324 cmdline: whoami /all MD5: 2E498B32E15CD7C0177A254E2410559C)
        - conhost.exe (PID: 5500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 4604 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",munlockRef@Engine@ScScript@@QAEXABVVariant@ScCore@@@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5668 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",mundefinedError@Callback@ScScript@@UAE_NAAVEngine@2@ABVVariant@ScCore@@1AAV45@@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- msiexec.exe (PID: 5520 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "BB30",
  "Campaign": "1685604052",
  "Version": "404.1346",
  "C2 list": [
    "47.199.241.39:443",
    "93.147.235.8:443",
    "75.141.227.169:443",
    "45.243.142.31:995",
    "79.92.15.6:443",
    "85.104.105.67:443",
    "89.129.109.27:2222",
    "86.176.83.44:2222",
    "24.234.220.88:993",
    "89.32.156.5:995",
    "12.172.173.82:22",
    "103.101.203.177:443",
    "70.28.50.223:2083",
    "98.187.21.2:443",
    "70.49.205.198:2222",
    "96.56.197.26:2222",
    "92.9.45.20:2222",
    "86.195.14.72:2222",
    "172.115.17.50:443",
    "100.4.163.158:2222",
    "80.12.88.148:2222",
    "213.64.33.92:2222",
    "113.11.92.30:443",
    "78.192.109.105:2222",
    "47.34.30.133:443",
    "122.184.143.86:443",
    "198.2.51.242:993",
    "165.120.169.171:2222",
    "88.126.94.4:50000",
    "82.125.44.236:2222",
    "117.195.16.105:993",
    "147.219.4.194:443",
    "80.167.196.79:443",
    "92.154.17.149:2222",
    "184.181.75.148:443",
    "95.45.50.93:2222",
    "84.35.26.14:995",
    "201.143.215.69:443",
    "12.172.173.82:2087",
    "50.68.204.71:443",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "79.77.142.22:2222",
    "12.172.173.82:995",
    "223.166.13.95:995",
    "72.134.124.16:443",
    "213.55.33.103:443",
    "183.87.163.165:443",
    "174.4.89.3:443",
    "27.253.11.10:2222",
    "2.49.63.160:2222",
    "92.186.69.229:2222",
    "69.133.162.35:443",
    "81.111.108.123:443",
```

```
    "12.172.173.82:20",
    "188.28.19.84:443",
    "90.29.86.138:2222",
    "70.160.67.203:443",
    "186.64.67.30:443",
    "5.107.153.132:2222",
    "125.63.125.205:2078",
    "2.36.64.159:2078",
    "71.38.155.217:443",
    "205.237.67.69:995",
    "70.64.77.115:443",
    "24.234.220.88:990",
    "96.56.197.26:2083",
    "70.28.50.223:2078",
    "103.123.223.133:443",
    "199.27.66.213:443",
    "83.249.198.100:2222",
    "94.204.202.106:443",
    "77.126.99.230:443",
    "72.205.104.134:443",
    "65.95.141.84:2222",
    "70.28.50.223:2078",
    "173.88.135.179:443",
    "220.240.164.182:443",
    "96.87.28.170:2222",
    "176.142.207.63:443",
    "12.172.173.82:32101",
    "70.50.83.216:2222",
    "161.142.103.187:995",
    "45.62.70.33:443",
    "24.234.220.88:465",
    "103.141.50.43:995",
    "90.7.72.46:2222",
    "76.178.148.107:2222",
    "116.74.163.130:443",
    "46.246.254.242:995",
    "70.28.50.223:2087",
    "12.172.173.82:465",
    "178.175.187.254:443",
    "27.0.48.233:443",
    "83.110.223.61:443",
    "184.182.66.109:443",
    "70.28.50.223:32100",
    "50.68.204.71:993",
    "70.28.50.223:3389",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "76.170.252.153:995",
    "69.242.31.249:443",
    "79.168.224.165:2222",
    "75.143.236.149:443",
    "14.192.241.76:995",
    "81.229.117.95:2222",
    "98.145.23.67:443",
    "98.37.25.99:443",
    "69.160.121.6:61201",
    "12.172.173.82:21",
    "75.109.111.89:443",
    "76.86.31.59:443",
    "80.6.50.34:443",
    "116.120.145.170:995",
    "201.244.108.183:995",
    "58.186.75.42:443",
    "68.203.69.96:443",
    "47.149.134.231:443"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.424621480.0000000002C4A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000013.00000002.425037724.0000000004870000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
decrypted.memstr	JoeSecurity_Qbot	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.rundll32.exe.2c60a28.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xe055:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9c7b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
19.2.rundll32.exe.2c60a28.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
19.2.rundll32.exe.29a0000.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
19.2.rundll32.exe.29a0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
19.2.rundll32.exe.2c60a28.1.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

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

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

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

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

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

Remote Access Functionality

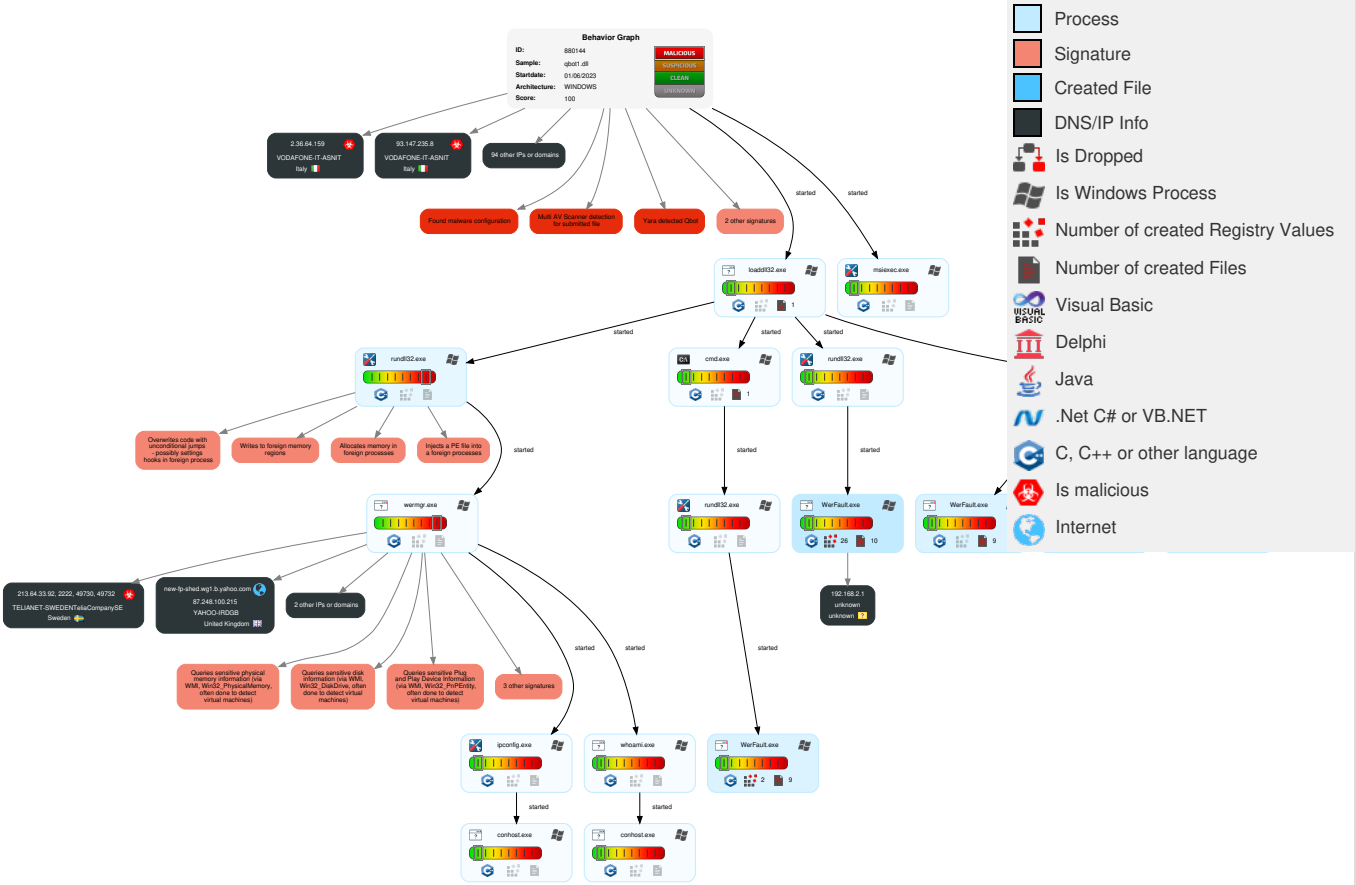
Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 4 1 Windows Management Instrumentation	1 DLL Side-Loading	3 1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	3 4 1 Virtualization/Sandbox Evasion	1 Input Capture	4 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 Obfuscated 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 Rundll32	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 DLL Side-Loading	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	3 3 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

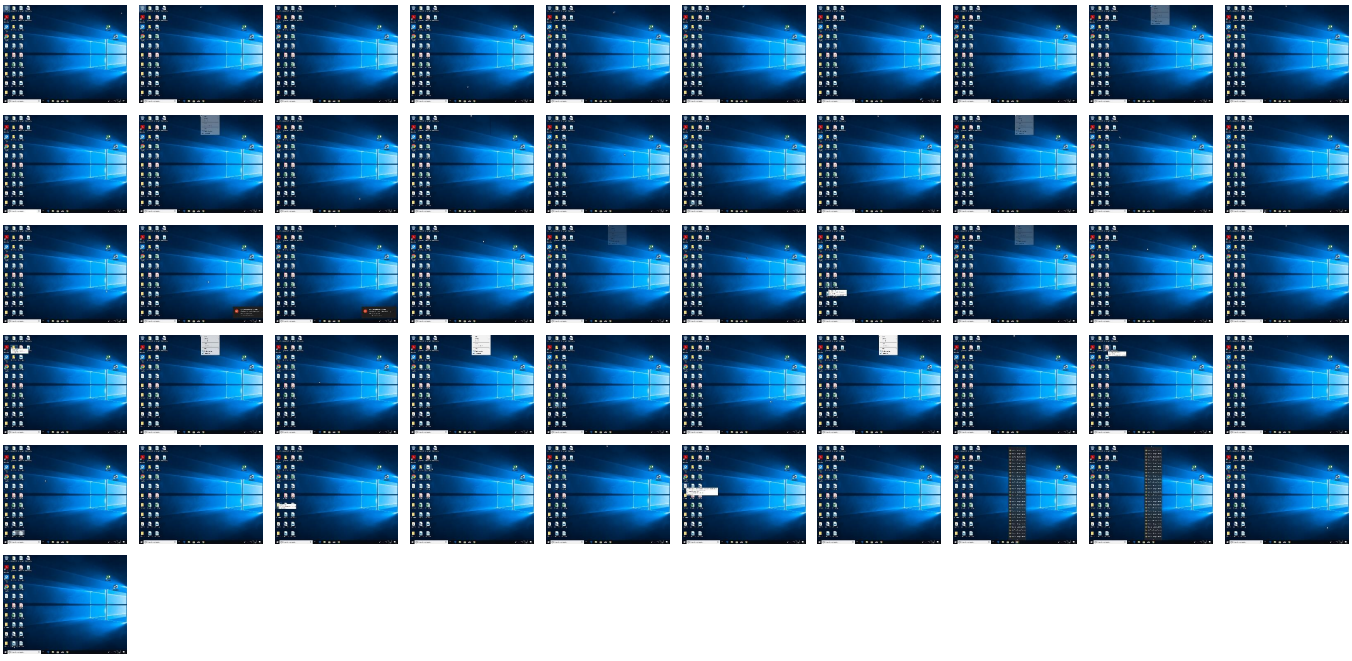
Hide Legend



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
qbot1.dll	13%	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://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://analytics.tiktok.com	0%	URL Reputation	safe	
http://https://analytics.tiktok.com	0%	URL Reputation	safe	
http://https://mem.gfx.ms	0%	URL Reputation	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Virustotal		Browse
http://https://d.impactradius-event.com	0%	Virustotal		Browse
http://https://openweb.jac.yahoosandbox.com	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	0%	Avira URL Cloud	safe	
http://https://www.clarity.ms	0%	Avira URL Cloud	safe	
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://d.impactradius-event.com	0%	Avira URL Cloud	safe	
http://https://start.microsoftapp.net/start?pc_campaign=UHF_Banner_15mkts&adjust=y9xgnyl_5sblqid"	0%	Avira URL Cloud	safe	

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
yahoo.com	54.161.105.65	true	false		high
windowsupdatebg.s.llnwi.net	178.79.225.128	true	false		high
www.yahoo.com	unknown	unknown	false		high

Contacted URLs

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

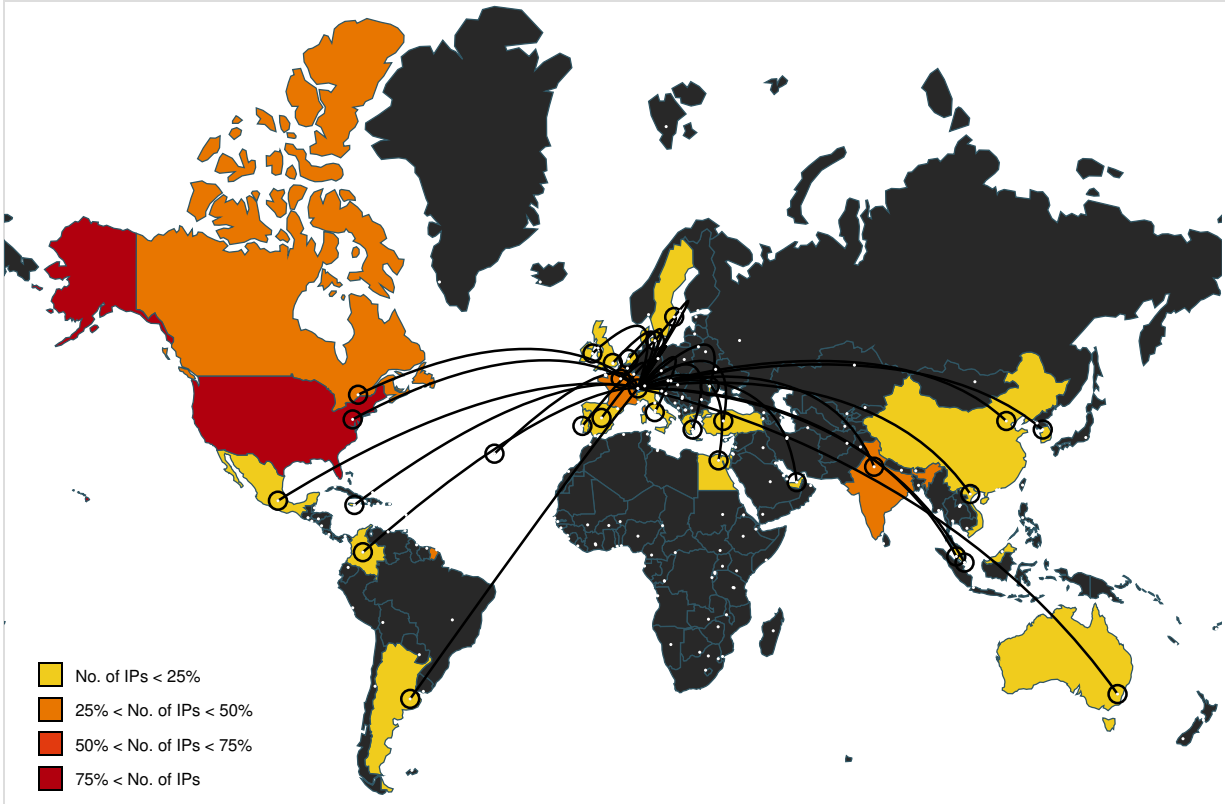
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/ss/rapid-3.53.38.js	J7NKSXWB.htm.30.dr	false		high
http://https://outlook.live.com/owa/	de-ch[1].htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/6lV3qkp5vhD2J.O5ha31Nw--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://www.onenote.com/?omkt=de-CH	de-ch[1].htm.30.dr	false		high
http://https://js.monitor.azure.com	de-ch[1].htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/fiFKhsorJ_.XzJNVa7HgsQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/h64YbbKcO2GsKYAy1QMRMw--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/cx/pv/perf-vitals_3.1.0.js	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/aaq/spotim/	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/p68hnTLk2asTrmg6nFL37A--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://www.skype.com/de/	de-ch[1].htm.30.dr	false		high
http://https://fp-graviton-home-gateway.media.yahoo.com/	J7NKSXWB.htm.30.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uu/api/res/1.2/7mz1gUykvPcUcalzuGE1WQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://openweb.jac.yahoosandbox.com	J7NKSXWB.htm.30.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/k8SbH9Gqa6W8a7JKyncC.A--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	J7NKSXWB.htm.30.dr	false	• URL Reputation: safe	unknown
http://https://lptag.liveperson.net	de-ch[1].htm.30.dr	false		high
http://https://search.yahoo.com/search?p=	J7NKSXWB.htm.30.dr	false		high
http://https://xboxdesignlab.xbox.com/xbox-design-lab?recipeId=G4E9FNSC&icid=mscom_marcom_CPH4a_PrideXDLcon	de-ch[1].htm.30.dr	false		high
http://schema.org	J7NKSXWB.htm.30.dr	false		high
http://www.opensource.org/licenses/mit-license.php	J7NKSXWB.htm.30.dr	false		high
http://https://analytics.tiktok.com	de-ch[1].htm.30.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html"	J7NKSXWB.htm.30.dr	false		high
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830424%7C0%7C0%7CAdId=-41;BnId=0;ct=1864049394;st=	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/H3vVA32ymLk3HFF8J_ZI5w--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://www.instagram.com/microsoftch/	de-ch[1].htm.30.dr	false		high
http://https://www.clarity.ms	de-ch[1].htm.30.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnssl.clicktale.net/www32/ptc/05d32363-d534-4d93-9b65-cde674775e71.js	de-ch[1].htm.30.dr	false		high
http://https://cdnssl.clicktale.net	de-ch[1].htm.30.dr	false		high
http://https://publisher.liveperson.net	de-ch[1].htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/4cg6h0vinH_o7ba.oxXthQ--~B/Zmk9c3RyaW07aD0zODg7cT05NTt3PTcyMDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/mzPB3eeJrxJuAn9uOhK0cA--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/aaq/nel/js/spotIm.custom.SpotIMJAC.modal.9d3270fa67932556c75baaed2c09c955.js	J7NKSXWB.htm.30.dr	false		high
http://https://d.impactradius-event.com	de-ch[1].htm.30.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/aaq/hc/homepage-pwa-defer-1.1.6.js	J7NKSXWB.htm.30.dr	false		high
http://https://start.microsoftapp.net/start?pc_campaign=UHF_Banner_15mkts&adjust=y9xgnyl_5sblqid"	de-ch[1].htm.30.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/2kRwuXH6fvmgKfpoQCf56g--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://onedrive.live.com/about/de-ch/	de-ch[1].htm.30.dr	false		high
http://https://s.yimg.com/aaq/vzm/cs_1.4.0.js	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/c3dObtZQiIqjZKMWzeYQcw--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lpcdn.lpsnmedia.net	de-ch[1].htm.30.dr	false		high
http://https://www.youtube.com/user/MicrosoftCH	de-ch[1].htm.30.dr	false		high
http://upx.sf.net	Amcache.hve.9.dr	false		high
http://https://schema.org	de-ch[1].htm.30.dr	false		high
http://https://s.yimg.com/uc/sf/0.1.322/js/safe.min.js	J7NKSXWB.htm.30.dr	false		high
http://https://mem.gfx.ms	de-ch[1].htm.30.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/5BZN9wyvjM8FfgniQrH0uw--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://aka.ms/yourcaliforniaprivacychoices	de-ch[1].htm.30.dr	false		high
http://https://www.yahoo.com/px.gif	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/6DI2hkBaEy3aroPxqBStjQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	J7NKSXWB.htm.30.dr	false		high
http://https://twitter.com/microsoft_ch	de-ch[1].htm.30.dr	false		high
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830441%7C0%7C225%7CAdId=11101911;BnId=2;ct=1864049	J7NKSXWB.htm.30.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-core-1.63.0.js	J7NKSXWB.htm.30.dr	false		high
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	J7NKSXWB.htm.30.dr	false	• Avira URL Cloud: safe	unknown
http://https://accdn.lpsnmedia.net	de-ch[1].htm.30.dr	false		high
http://https://www.linkedin.com/company/1035	de-ch[1].htm.30.dr	false		high
http://https://www.xbox.com/	de-ch[1].htm.30.dr	false		high
http://schema.org/Organization	de-ch[1].htm.30.dr	false		high
http://https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	J7NKSXWB.htm.30.dr	false		high
http://https://yep.video.yahoo.com/oath/js/1/oath-player.js?ypv=8.5.43&lang=en-US	J7NKSXWB.htm.30.dr	false		high
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	J7NKSXWB.htm.30.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
27.253.11.10	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
80.167.196.79	unknown	Denmark		3292	TDCTDCASDK	true
92.186.69.229	unknown	France		12479	UNI2-ASES	true
89.32.156.5	unknown	Italy		48544	TECNOADSL-ASIT	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
125.63.125.205	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
165.120.169.171	unknown	United States		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
79.92.15.6	unknown	France		15557	LDCOMNETFR	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	true
98.187.21.2	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
103.101.203.177	unknown	Singapore		133136	MYREPUBLIC-SGMyRepublicLtdSG	true
117.195.16.105	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.204.202.106	unknown	United Arab Emirates		15802	DU-AS1AE	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
98.37.25.99	unknown	United States		7922	COMCAST-7922US	true
5.107.153.132	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
81.111.108.123	unknown	United Kingdom		5089	NTLGB	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
54.161.105.65	yahoo.com	United States		14618	AMAZON-AESUS	false
87.248.100.215	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
85.104.105.67	unknown	Turkey		9121	TTNETTR	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
2.49.63.160	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
116.74.163.130	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
116.120.145.170	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	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
47.149.134.231	unknown	United States		5650	FRONTIER-FRTRUS	true
82.125.44.236	unknown	France		3215	FranceTelecom-OrangeFR	true
90.7.72.46	unknown	France		3215	FranceTelecom-OrangeFR	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
46.246.254.242	unknown	Greece		1241	FORTHNET-GRForthnetEU	true
45.243.142.31	unknown	Egypt		24863	LINKdotNET-ASEG	true
70.64.77.115	unknown	Canada		6327	SHAWCA	true
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
213.55.33.103	unknown	France		49902	SRR-ASFR	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
47.199.241.39	unknown	United States		5650	FRONTIER-FRTRUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.176.83.44	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
93.147.235.8	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	880144
Start date and time:	2023-06-01 21:22:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	qbot1.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@40/37@2/100
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 72.9% (good quality ratio 42.8%) • Quality average: 41.7% • Quality standard deviation: 40.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 20.42.65.92, 20.81.111.85, 20.84.181.62, 20.103.85.33, 20.53.203.50, 20.112.52.29, 23.36.225.122, 178.79.225.128
- Excluded domains from analysis (whitelisted): www.microsoft.com-c-3.edgekey.net, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, e13678.dscb.akamaiedge.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, microsoft.com, www.microsoft.com, wu-bg-shim.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
- Execution Graph export aborted for target rundll32.exe, PID 5044 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 6336 because it is empty
- 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
21:24:00	API Interceptor	7x Sleep call for process: WerFault.exe modified
21:24:06	API Interceptor	1x Sleep call for process: loaddll32.exe modified
21:24:17	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_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_1995889c\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):	0.915002607621147
Encrypted:	false
SSDEEP:	192:C5Ai90oXXHBUZMX4jed+T/u7sdS274lt7c:fiTX3BUZMX4je2/u7sdX4lt7c

MD5:	E3B8E452B6905834223D17CCD4EEE909
SHA1:	E0919958374592CF3D504023D49D034AEE63B6B7
SHA-256:	EDCE1586E87A1EB14974726222CED71ADFC19D7E5F8BBEE714B79D525F3A5681
SHA-512:	D908C996F6C99413668A3C891F2D2EB8788154D6AC1B511737471D2B97B8E883B8AD57B2307ED0D2871AE2D8AD351E7EBE5D9AB7FA76BEE0157977090B89B2A B
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.7.1.7.1.3.8.0.6.....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.=.1.3.3.3.0.1.5.3.4.4.8.5.6.2.0.1.2.0.....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.=.f.1.5.0.3.1.b.f.-.2.8.d.2.-.4.4.c.2.-.a.2.5.8.-.1.b.4.1.4.f.6.b.2.4.e.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.e.1.8.7.3.9.8.-.4.3.a.7.-.4.6.6.8.-.9.c.a.7.-.5.9.e.d.b.6.8.2.9.7.5.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.f.4.-.0.0.0.1.-.0.0.1.9.-.3.9.8.9.-.8.0.1.1.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b56739\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):	0.9146863971413854
Encrypted:	false
SSDEEP:	192:M+v9Yi80oXwHBUZMX4jed+T/u7sdS274lt7c:vlYiaXYBUZMX4je2/u7sdX4lt7c
MD5:	6C48A77D55D5EEF62D423BD585BD79A5
SHA1:	9B17CB0ECC3B6A61133A37AA4BC3503BA7E61382
SHA-256:	286848A90FA4AA5205387B4EFFBDDB6F7D82D53757E63B3F3B3B87AEA5E28811
SHA-512:	5D90873B5839B4CA27358E04E8F020250FB8924876650BAD0B0107523AA7BFF79B33FD7E63B368276A37826FA3C9064DA7AC8EFB5CFEFA83B1CF0C7AD58FBE5 3
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.3.8.2.1.2.0.1.2.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.5.3.4.3.9.5.5.5.7.7.0.2.....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.=.2.5.d.8.8.f.4.c.-.7.b.4.9.-.4.8.e.0.-.a.1.e.6.-.6.7.5.2.0.2.8.8.c.8.1.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.8.a.9.2.9.3.1.-.5.d.1.3.-.4.0.6.2.-.b.1.d.a.-.0.f.1.e.5.3.3.2.7.f.5.a.....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.=.0.0.0.0.1.8.7.c.-.0.0.0.1.-.0.0.1.9.-.c.a.7.1.-.0.9.0.c.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b96630\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):	0.9145207095088187
Encrypted:	false
SSDEEP:	192:oiVi40oXrHBUZMX4jed+T/u7sdS274lt7c:hVi+XLBUZMX4je2/u7sdX4lt7c
MD5:	50B09CAFDF20321439A6DB4B7C3EED2E
SHA1:	C75DBD7124FC2D614EB0F5C4987D8299230BBD68
SHA-256:	B5D6BA083F1D06290A6E57A30F94B96ABAC76F819C7D2649F9C8C0890DF420CE
SHA-512:	83479AA85CA8DCBC45F544AA58353C04DD3800789305D78C99E98270C06070C481AE13A3B286F253DDCB9BE36BC5E847E028F52D172EF1A79ADF3BEA6283E5 2
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.3.7.9.4.4.1.2.5.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.5.3.4.3.9.3.5.0.3.7.2.2.....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.d.c.2.5.7.0.0.-.5.1.e.1.-.4.a.5.a.-.b.b.5.f.-.8.0.d.f.5.d.f.9.3.f.9.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.3.e.d.b.3.a.a.-.b.9.3.7.-.4.7.3.1.-.9.8.0.0.-.5.5.c.2.7.8.7.2.e.1.8.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.c.0.-.0.0.0.1.-.0.0.1.9.-.0.1.f.d.-.0.5.0.c.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_192989f4\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):	0.9143409653771047
Encrypted:	false
SSDEEP:	192:VPRiG0oXl4H4DmIwspjed+T/u7sdS274It7c:DigXlg4Dm9spje2/u7sdX4It7c
MD5:	2D682A8224D537C0F111276D03881A4E
SHA1:	CDF1E2EA63E25AD49550A5A55DC9C68AF2CE8C8A
SHA-256:	9736F9B5427102B930D6C65724CF186B8E185F3C0928466509B337D2FA805A4C
SHA-512:	BAAE4E8F98B915A4F53C9EE10A3F68CC655FAD6D2945156C67D807200E2C14A99F9FFC97CDB52E279FED877BDCD8BABA7EA99FDCF78696FEBD10B1595845A090
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.7.1.0.6.6.4.9.3.....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.=.1.3.3.3.0.1.5.3.4.4.9.1.5.3.5.3.3.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.1.2.7.9.0.9.0.-.5.4.e.9.-.4.b.2.3.-.a.9.e.b.-.9.e.5.4.1.d.b.5.d.c.a.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.4.7.7.3.e.a.8.-.a.e.e.2.-.4.f.3.d.-.b.3.3.3.-.4.1.2.3.e.e.b.5.3.9.5.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.3.4.-.0.0.0.1.-.0.0.1.9.-.2.7.c.e.-.8.9.1.1.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1a9588cb\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):	0.9142965009322384
Encrypted:	false
SSDEEP:	192:GqociH0oX84H4DmIwspjed+T/u7sdS274It7c:bJi5X8g4Dm9spje2/u7sdX4It7c
MD5:	A6F228A8887653F4BA5F9EE3F037A78E
SHA1:	FD992206DB72C573625DC207D44ADEF4245F7B03
SHA-256:	0D1B7924D7D6D13A96B24D0DB3491107CEB20C94092B1D09B1D98F42290E7D2E
SHA-512:	350EB06778C6FB662115620D21CB6AAB2BC2CA2137A17652A60C5ECE86BE9CFBA1CF84B4F6B9D06029E8770E8EDFA319F84C58980F61C4BD34FE115E4AB5C2A9
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.7.3.7.0.0.7.5.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.8.8.0.7.5.8.6.2.....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.=.0.6.3.e.b.3.8.5.-.d.0.6.e.-.4.c.a.1.-.b.a.d.d.-.b.9.3.c.b.4.5.a.7.e.6.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.b.b.4.2.4.c.7.-.9.5.3.d.-.4.8.1.8.-.b.e.d.1.-.7.4.4.f.9.0.6.c.0.2.e.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.4.4.-.0.0.0.1.-.0.0.1.9.-.8.b.4.7.-.8.5.1.1.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1bc56fb5\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):	0.9119922442128534
Encrypted:	false
SSDEEP:	192:psji00oXy4H4DmIwspjed+T/u7sdS274It7c:+jiCXyg4Dm9spje2/u7sdX4It7c
MD5:	F77BD1F387C84B185AE1C22F902F7196
SHA1:	B0097CB3DC0802749D5FC34A630BBD84B5D94D23
SHA-256:	DDA783AD97B60EC2C3AECAB85B81DE87F8109A4BFE14FE98CEA23441E907BD30
SHA-512:	31B5F7864B8049D35FE66018B833ADD7A1175F5C374BEBBC0E4F19BA0D8BBC7376923F7DF0FE514B35C4E4F1DBB89BE1B372191D26ABE324700787DF7DD476B9
Malicious:	false
Reputation:	unknown

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.0.8.9.7.5.5.6.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.2.2.5.7.0.6.0.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.6.0.d.b.e.0.f.-.a.4.d.c.-.4.7.b.e.-.a.a.4.8.-.4.6.5.8.3.5.9.2.6.d.d.d.....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.=.7.9.3.6.5.3.8.9.-.3.6.f.9.-.4.e.b.3.-.9.a.d.4.-.f.e.7.3.8.8.4.c.d.d.7.f.....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.=.0.0.0.0.1.3.b.4.-.0.0.0.1.-.0.0.1.9.-.9.e.8.1.-.d.b.0.d.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1be17998\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):	0.9142282591630437
Encrypted:	false
SSDEEP:	192:aoZiQ0oXp4H4DmIwspjed+T/u7sdS274It7c:ZZiGXpg4Dm9spje2/u7sdX4It7c
MD5:	E0805D5A621EDF99019E314B5413ABD1
SHA1:	C6052D07A64F462985B1A9F85288677BAAA35118
SHA-256:	D58F70CE84BE05FEE341E245CDEB7D7594D92420C5F2B6F5E0A1876191E74888
SHA-512:	824BCDEB10D50FD4AABD35172C9ECE02886F98A455D387DBA80D42562BD2D46FD012AF9F6FD296BDB94750951AA68C120714C6E7E5A3E9755FFA9505DC6E737C
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.3.6.2.8.8.7.5.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.5.3.4.4.4.8.7.8.8.8.1.2.....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.=.e.d.6.3.c.f.2.0.-.b.5.b.c.-.4.6.e.0.-.9.c.6.2.-.1.5.b.c.8.f.f.c.1.c.b.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.6.3.5.a.5.a.3.-.a.9.5.3.-.4.6.b.3.-.b.b.2.3.-.c.5.e.e.c.f.5.2.e.b.7.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.8.c.-.0.0.0.1.-.0.0.1.9.-.b.7.7.e.-.a.c.0.f.0.a.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:23:58 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37500
Entropy (8bit):	2.1920623787102325
Encrypted:	false
SSDEEP:	192:oMduyywZLCQHjPaSO5SkbCf5gZeTOjhs3QeD18HbdKbn:jhit5LbWqZHs1D18Hbs
MD5:	CD5FDCEB57FFC783A103B7A8045C1173
SHA1:	68EEA24E1A85933E53442AF9490B31DCCD08B3AC
SHA-256:	25404AA60669C0F070FED19F4CAC7DCFAC0532AF97523C713F5344C6C90C450C
SHA-512:	29D3150A5616EC882641440FD9F717BB0FF3B5CD66C96D4D0AFD672C0B66B8752CA9ED4CD9B34178FD7907C89A258DED039D2D02A29436D0BFD4250EC65A72F
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....d.....I.....).....T.....8.....T.....|x.....U.....B.....GenuineIntelW.....T.....nyd.....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\WER5C4C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:23:58 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	42512
Entropy (8bit):	2.1368984728128018
Encrypted:	false
SSDEEP:	192:o1FKuhMYGO5SkbBBArje/MNpq9jIt4VMqK6uQz3jHoEhcnr7:Qx5LbBBAu/MNKjIWqrQz3sf
MD5:	218611254C62CB2742F45C2FB5BD409C
SHA1:	198A24860EEB9EB1FF629DFEE5FFFBE5C1248C33
SHA-256:	BAFB4607D780B22982B5B6CCAFD314C067C5FFDB804753C71ECECA2A29C0A67A
SHA-512:	DA108F7D8D7C1714EACB02168808C9C170EF42615591345153918E1DD4328D4D3D25EBE186031705B1779EC0D851E430433FF2E48BF3A441B7A4FDF502E455A8

Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....,.....T.....8.....T.....P.....0.....U.....B.....GenuineIntelW.....T.....|....nyd.....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\WER5E22.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8352
Entropy (8bit):	3.694869168823069
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFy6W6Yct56igmf8tSUCprs89bdYsfdf/m:RrlsNiw6W6Yg6igmf8tSFdLfd2
MD5:	766D311EC9B8E1C07D6BA05A2A18757E
SHA1:	1DF2DE8A906AC9C9D8FF0C777741374C3F39E19F
SHA-256:	D88A94CD82A5E157B1D1A1BFD3A05C8B0BFCA8708D1BD5F3DD52FA317B3AD938
SHA-512:	2F05FA2582D945EE05C94961E8E9CAD1383E631375F048320FDD25059094EE6B02E04E3EE0596188A21D535B4A73BE38ED02C6FB796FCFD571FDDD8D5F4D6E4
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E90.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.4846523256031325
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9//HWgc8sqYjHAa8fm8M4JCdsPMFg/lKj+q8vjsP74SrSpd:uITfwc2grsqYLAvJ95gKm7DWpd
MD5:	F6B91D5FB4A19CFE26B52C6C9DF56AFF
SHA1:	53DA30755A4DA40EA3BB0D2834798D29A1BC8692
SHA-256:	692C54B535D1828EA09BE9C41D2657E2ED6FEAB496B4CE314DCF216C06179CDB
SHA-512:	27FA834A8F5198F04B13CDAB407416E73DECE469442A560F228BFCD78D4259EA9369CC35A375CBAB390045438B68C8BA2B812FFD013C8364EFEE399C37E1E52D
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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\WER5F0C.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):	8348
Entropy (8bit):	3.698547898786485
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiX2606Yiq6R8gmf8tSUCprd89bdRsfn3/m:RrlsNim606Yv6qgmf8tSmdKfnO
MD5:	273217C16BF0FC497F9E5522BE51B0C2
SHA1:	DA8208F18E32E6387C38B1D13EA60B00B07436CA
SHA-256:	7B314F8DC52E6EBF0BE813108545C52008F5F931A8D8FECD30BF5E3BA9FE4730

SHA-512:	DB3344A17F071B61FA7F9AB7ADC0CEE03B6AFAAF0C5487DA2B637312324B668B027EF103EBE36A9EEF063F1ACDF36FF6B36B56AC5BBEEFB682C41DCA252EBC08
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.2.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F6B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.483156697569828
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9//HWgc8sqYjHPb8fm8M4JCdsPMFH/C+q8vjsPt4SrS4d:uITfwc2grsqYLPYJ9+CKmtDW4d
MD5:	BAAF2F7320FC416AFF3D044D387FEBF8
SHA1:	9B518E2535981828845E5C2A0016449AA53BC003
SHA-256:	E6223078BA4FBD4A752965D844A1A57C4C39BC80E55CCEA478394733D8A6E73D
SHA-512:	F2298E51D9CA6769E6E25C61B215B921E8B9B093F5E907660D4B2125F775E293E26806179A3762253613F68C0CE99BC7C071602530E8D67BA6C7BF896735009A
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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\WER66BC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:24:01 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	293204
Entropy (8bit):	1.5462880708340312
Encrypted:	false
SSDEEP:	1536:2mAhOU6FQwSjU33x+yeoTnVTUXTqxl5jzJ9Cm5V3J98ze1VgZjpP9+tR6ssEBOVo:HNTnC4PFdlGa2s
MD5:	AB8BA3EDD0F75B40AC0D829563C21FD3
SHA1:	249D73D37E921C84135A9BDAD2A32898E3807C7F
SHA-256:	CA79B082EC2BF44E390369083350C4CFA6B01A16425E21606EB8AA90CFDEF3EA
SHA-512:	B99169F5F53C5CDF20CEE20B370DC8BCD2057AAC836264521FB1E68C68F2A1904DFF0A49B7F46D30836CCBA7D31E71FD990DA54E880E7146350EF11F80E8317A
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....,.....T.....8.....T.....,.....0.....U.....B.....GenuineIntelW.....T.....nyd.....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\WER69DA.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8352
Entropy (8bit):	3.692737898158134
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4062y36YcA56/gmf8fgSNcIOCpD789bOlsf6am:RrlsNiL62y36YX6/gmf8fgSNcPO+fe
MD5:	A0002A1104F4524D7E9CCF59B7C759F8
SHA1:	CB4FCF05FCD37126A10EAA7C226866A304BE7BAC
SHA-256:	29CE464BA14B96F2CD217AEF8C92201EE6C3170AABF62852583CBF256E2557AA

SHA-512:	67EDC29094A9C4F11BE54F59F68BE31A3D5DBEF2FB6D6DED6914EF0FF732D24A59C51F3F853BB8BED477AADAD4251BD79FBE57F21A25A56893179CF21CDFD9FA
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.0.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A1A.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.483416044971313
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9//HWgc8sqYjHy8fm8M4JCdsOSFIL+q8vjsOR4SrSzd:uITfwc2grsqYLnJWKdDWzd
MD5:	3F485836A957823403FA2FC947D91EF4
SHA1:	473970BB2E32EF57189D9997FB261FDACAA10599
SHA-256:	6432EEA9B2D9D46E062E44F24CE81967B8858E497B81361932359492 43A6E301
SHA-512:	6AD7C4DC83AA069726CA21835A1B346F3D33F946A5CA66E3F194465E659C98F10A69B6FDC82700C531672C158A67B84416C4C6769ADE37B9C3A087ADB9F92BE
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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\WER716B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:24:03 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	293668
Entropy (8bit):	1.5943164474368186
Encrypted:	false
SSDEEP:	768:J4VbIipMGTpcs12zBnBaDbW/TW/q7hzXBAETtjELfwmHb68W2sSfDAS/z2e76c3G:W9Wz3EQzTYjBhiTpYAM0
MD5:	CE257CE8A09C98557CAB82FA6575987F
SHA1:	107D2FED650A84B1030EFE93B01439D87101D342
SHA-256:	8719820F273D1D1039E3EFEF1899ABB4DA079C7E5E28DEEF30C210F21969A992
SHA-512:	945E0A2D73FC24BFD215E8823D630CE1DEDB3EF1C55CED0EE5A09E4365719F4401629A7AB2F9F25824E59F09770545974861AC67BC0C160BF60F3567C964C02
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....,.....T.....8.....T.....ta.....0.....U.....B.....GenuineIntelW.....T.....nyd.....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\WER741B.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8352
Entropy (8bit):	3.6956936206982727
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiSa6D6YcA6vgmf8fgSNcIOCpD089bzzsfz7Rm:RrlsNif6D6YL6vgmf8fgSNcSzYfzA
MD5:	0CCAABC752A1E97888D29DC2DA964062
SHA1:	D5200551990229A87AF87700F5A7E9A03380E48B
SHA-256:	A9B426F98E4DC8C03D623F6784CEFA3145D4F5A74C69C4678E25A7302D4D5711

SHA-512:	32B60A4A1B7228409E4FCAF132E6771B3E27AF318179003B74DC3C790F9E106126DAA22363BE7B6CE459804540467549CC01A5AD6CCA45EBDC9E7BC80D7F0FB
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.7.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER745B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.481111792575972
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9//HWgc8sqYjHf8fm8M4JCdsOSFxj+q8vjsOf4SrScH6d:uITfwc2grsqYLEJBjKjDWi6d
MD5:	CCDECBF336F174545F9583438F0AB11E
SHA1:	31077430104E1CA056423AF77B0FFE4AC7F3F3E1
SHA-256:	FE7F847FBFAB077C419B12B8A0D6ED2628AB5DE0B4ACDE038C18B51BA0B00189
SHA-512:	381B7E543F4C59FF708148A2A8F433C9310E07E8AB11D995C3B26737671BAF1DB30E1AE488589F004EBC49254415386A877ECF9CE349E4BFB11EEE3BC1C1DE0A
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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\WER7F07.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:24:07 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	293240
Entropy (8bit):	1.5589987345084229
Encrypted:	false
SSDEEP:	768:cVbkmd4ARMzDx43kQhvhLgwHNSVh7ff4Hlh2zSdOcfXPSKJuzEkrXHqADaE+tuC+:fiMz943kzD3BArSl1ZZywQfA6UL
MD5:	DF14A3664018A926DAF4B646CAA04F5B
SHA1:	B30B39B12A146B9FAAF47E6D1E3649313B7CB66B
SHA-256:	04EA3FE19640CF0003275515F4380108C1097C2D898116315FD3E88B59627F67
SHA-512:	48DB1F37CA02340296F7321146CF972FCAFCCC9E904B4B216430FDB42606224B7743D4003F11C88F80A48EB9B17F8160B3DBF7F08881C0A13BC6E7D877A036BE
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....,.....T.....8.....T.....,.....0.....U.....B.....GenuineIntelW.....T.....4....nyd.....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\WER7F45.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:24:07 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44420
Entropy (8bit):	2.015944415298908
Encrypted:	false
SSDEEP:	192:BTEsHu6MYOErO5Skb9X9U1Su/lYbukYzfo8TZoHdI59cHVQOTzJ:695Lb9+1nevYzCHdIzcnv
MD5:	A3F37405769F84FF3811DFACC3C26D8E
SHA1:	BAF8A14C949D847F034C236A4FC2908E606087C0
SHA-256:	38235CA2CFF612B9F335059DCB02C0281B1B246A247859B2AE6A7CBCE3C87A2B

SHA-512:	70824F60A8AD046D8581FA7148EA5DA504679C1712E7ADB3D4AC6D04A6966482403ABF068396E0F9DB318518B24DD11C733E996C35A5EB729F1D5C740FF64F3
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....,.....T.....8.....T.....0.....U.....B.....GenuineIn telW.....T.....nyd.....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\WER8011.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 04:24:07 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	296044
Entropy (8bit):	1.5475407768344807
Encrypted:	false
SSDEEP:	768:/VbatbiK0g56qoX6fZ7F2eVPkiT3Mx5Rcqb6cWCNxsYDGxDoudE7OwkDhkB+kbOT:sFiL0QXxytbB7d
MD5:	ADA5C3FB3C0D07500E77F0C4B2B425E3
SHA1:	AB213A962B004A5D4D34C70CB5223AD7D54BF601
SHA-256:	FDCD4145505CB3A5EC374D55C64ACE1966C310A11BC365C8E82ED933E3BA7C8C
SHA-512:	B8ACBA6C37930F8DB5F7C2EB32C8D21CFC76989388FF7D6DE730DBAB88F01B6224FF962F1ADF2DF3C47EBD8163285A5B134B4E961B62B4FC1B6D0218CE79A 5E
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....nyd.....,.....T.....8.....T.....j.....0.....U.....B.....GenuineIn telW.....T.....D....nyd.....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\WER813A.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):	8346
Entropy (8bit):	3.6945834939030493
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAO6l6YcW6zugmf8tSUCprV89bCb0sfQcjm:RrlsNip6l6Yl6agmf8tSeCbnfT6
MD5:	64ABBCC421F6DAF7A50B19F079929E3C
SHA1:	331D3FF5B4054E55FDC93A31C56FB1160B299AC1
SHA-256:	18E7CF372C5728BAADADFBFB5A255EDB00CC93EFF05F06CB57B74B2588BEE3B5
SHA-512:	CB20536C2D076A428D2D42A4B493876D1A2F7A3FA208BEAD44154EB7CEBA311635DC4915AC0FCE31C644868AE4E7D8D8D2370940965DC6937FF2DD7E1130C2 E0
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.5. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8199.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.487572544770219
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9//HWgc8sqYjHY8fm8M4JCdsPMFC+q8vjsP24SrSud:uITfwc2grsqYLVJ9fKm2DWud
MD5:	4E00FF04EF946AE380CF2F321E733A79
SHA1:	E86C208536C78DBF8FD42DC3826A3B2C81014D0B
SHA-256:	2C6F1B6997D9467B87B59F832A9ABB2514BBF38BE9F1B6D86F05FBC3F31699E7

SHA-512:	12A8CB02F629F69C6C7561CE746DBD236BC18CD4A7BD59886660DED33F80D8CB9C5ADBAFD317A4F2CF9E8B9104E5663644FA4483A6CDCF0033C4DB413EF0945
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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\WER832E.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):	8346
Entropy (8bit):	3.691880415628122
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNicL6s6Ycc6zugmf8fgSNclOCpDU89bfxsf1e1m:RrlsNig6s6Yf6agmf8fgSNcyfqf1t
MD5:	D490F83E2FC1BE0F92AB629FC6F16A3B
SHA1:	2465DE9DD3D6F380E7722860292685992CBF7C44
SHA-256:	26DDB140CB96FA3BEE8F9956620152D2C939081AE60E1B6A98A4095D891EEC20
SHA-512:	0AB42F3A9D8A93FD2188EA243962D1D3392671881C6DD745D260B3F9DCDA2F6E8D4AD8A6FC734760F5E506BC3FC0610DAE2DF4B88B0BCB028E32C5253D8AE03
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER838C.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):	8346
Entropy (8bit):	3.693600944583375
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWp6cje6Ycz6zugmf8fgSNclOCpDZ89bfUsfY1m:RrlsNi46cje6YA6agmf8fgSNc1fHfH
MD5:	FC6D470526A0C5A459539470D47CC7A7
SHA1:	647475BDD7C0867DAA24C7B86A73E7167B58C0F1
SHA-256:	9E0EBB5FBD2ABB782B579198FF85868647B41D88637B201B957C6DD675569FC3
SHA-512:	0D8AF0F891BD5560DCAAB16F137C708BBAA7638586D86201C15FB487F4D2436BAD4477A1AEA7E16F5B301466B881CB7273AE2B909C7F0A5C87E4E711D1493098
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER838D.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.4819139752559645
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI9//HWgc8sqYjH88fm8M4JCdsOSF++q8vjsOc4SrSxd:uITfwc2grsqYLBJuK4DWxd
MD5:	D81F383B9510748543996EE07692F222

SHA1:	C451BDE607B9A888128AC3EED1F8949BF4FE40C2
SHA-256:	69F8AB8614102F301FAD416D91BC8C94E19924AFBAE87860A12BE11322B1D62B
SHA-512:	1DDA29560368DA5A44497510B38DC13D8B6066BF63A71F4973F2596B33879E4B6E89177EF1C59D7EB1FCBDC162B9D69AA3899A7DD7832CB9AE089943028F5B6
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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\WER8449.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.480053765611426
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWl9//HWgc8sqYjHus8fm8M4JCdsOSFN+q8vjsOv4SrSUd:uITfwc2grsqYLuRJ9KbDWUd
MD5:	0164AF8535F27C20EA89F7C465C0FB97
SHA1:	63E6DF600ACF3CE5F2D1FED9A614AC93FB37BB3A
SHA-256:	B127F093538A40981B525AC4629823CFF1A7F7FD2D86F21611F97B5EBD7D4268
SHA-512:	34123901DA539AC3165E742CFA2D765BDEDE94D32F56F2FC5C53ECD0614EDBE8D76E0B330944C0236CF1C2C646644A0089EAD6BE3C3496FB3F5A7CD52ACA64A
Malicious:	false
Reputation:	unknown
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="2067214" />.. <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
Reputation:	unknown
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.I....,{...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):	290
Entropy (8bit):	2.928044663379677
Encrypted:	false
SSDEEP:	3:kkFklbWJEvfllXIE/qSvmtlJ6pFRltB+SliQlP8F+RlTRe86A+iRlERMta9b3+AF:kKOoNN+SkQlPlEGYRMY9z+4KlDA3RUe/
MD5:	A9EB58CC94E193F7CF4DF5789BD9A99E

SHA1:	DDAE2B599C7F6EB89B70706416A02C096207F8C5
SHA-256:	55B0CD0EC6EF8DEF5AB2C5300AD26209F96D8A9300A8BD0AB013D0E93505A560
SHA-512:	404101CB66D680CEE2296DDEB3C91B14BA8AA5CB6C3C583767977F346C2562729E0FF131B1698E28E93AB1B74955FF48E96F8BDCAE1DD66A225763FD2A77779 5
Malicious:	false
Reputation:	unknown
Preview:	p...... ....+.Z.....(.. ....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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\J7NKSXWB.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, ASCII text, with very long lines (64945)
Category:	modified
Size (bytes):	881416
Entropy (8bit):	5.578898933095815
Encrypted:	false
SSDEEP:	6144:bWYjR8+d18F3OYRIBK1WptCLhQtICvOWBCEn+l4pz2BEXUAz:bXR8Z3OYWNp0WOoCEn+WnUAz
MD5:	ED2EC7A6789ACF6FDC00709B2A3135A6
SHA1:	1E6C7E4BA0DE7783E0D779591CC5DB579F9EA30C
SHA-256:	6795223FEC92ACAEA98722BBE2DD6A969C04379D6811B5FD3D9159737150469A
SHA-512:	519B4A7A6B0D6E2F0F4D94CE16DAABDDB05B3623E77D32305FC285DB1CC28597B5E87B93F1DE89D44B6EB0AA943323A05D40AC51A73ADC44E4D3E809419A5 91F
Malicious:	false
Reputation:	unknown
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=2dc40bb0e8f14317f5506 4956635585ba1e88d32ab41e65fae69eacc39bdd39b>. window.performance.mark('PageStart');. document.documentElement.className += ' JsEnabled j senabled';. /**. * 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 b eginning. Discover m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\de-ch[1].htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (3929), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	148097
Entropy (8bit):	5.02462840216527
Encrypted:	false
SSDEEP:	768:m1gCPecqKIRxUtMqNPnOwMO4q68oGlRI5lH9D12lBYc2U9a9H9Z959APA7B0M+op:yghkGwMO4q6cI592tKdvPXFh030
MD5:	AE04B92E6A413F74684B96D0EC898634
SHA1:	4CE92CF45ED02D036D38B1979AD4462F44A113E7
SHA-256:	2B15A2FF73C2DF9E2D2D5D76336D0A86D92F5E7DB3F103456809F0CDAE6C4BEA
SHA-512:	368CF432228AE7E8F92B266B3FA0974FEC5D4E0768AAFC362BB6C42AA26244F1D564365EE8F90702652DD921E7CA1B5CC04FD4EC358A903990439127713F1BC
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML>..<html lang="de-CH" dir="ltr">.<head>. . .. . Start of ADDITIONAL DEBUG INFO ** cv.html **.. CVToken: CASMicrosoftCV101a59d9.0. End of ADDITIONAL DEBUG INFO -->..... . . .. . . <meta charset="UTF-8"/>. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/>. <meta http-equiv="x-ua-compatible" content="ie =edge"/>.. <link rel="SHORTCUT ICON" href="/favicon.ico?v2" type="image/x-icon"/>.. ... . <meta name="robots" content="index, follow"/>. . .. <meta name="template" content="mscom"/>.. . <meta name="awa-canvasType" content="web"/>. <meta name="awa-isTented" content="false"/>.. <meta name="awa-pageType" content="MSCOM Home Page"/>. <meta name="awa-pgtmp" content="mscom"/>. <meta name="awa-pageId" content="4bca0c3fec9ac6f60e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\t5[1]

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	ASCII text, with very long lines (784), with no line terminators
Category:	dropped
Size (bytes):	784
Entropy (8bit):	5.948782853717203
Encrypted:	false
SSDEEP:	12:HDY9UxUpcJOmjBKADm01mOcZp1jU5WPH0ubmK9iOsz4Kd:HDY2xmbOlmKcOiH0Gsz5
MD5:	FAEBE201B102D79B40ECB6399B07085F
SHA1:	CA35D55163A539B8999CFDB3E34CFC0B8978EBEF

SHA-256:	50CA1BF3024A6F7623412BBCA492A8C8E64BA3B9D3D7E8F1AAD1977EEEEBE971
SHA-512:	42FD52D5DA5FDBD071A80E34CD046A092C83A76733E62CD46F0FF1D59E1F6646070C133452689345B713755E02E9BAD60103F1F564AB5B181371DA33704BCFF4
Malicious:	false
Reputation:	unknown
Preview:	zN/wXnY7/aDNWws3Oh0RkXC0oDZ4fsPEWsr4nknG45X1yabwi7Z/pJMYDMOTVF0G7sWJE4ONSOpHNm6VaJRntEwmLBNzgSjMHQzhuEsClaLM8xR+j8cH0DzD FJLelOAi2hqfXzkmZimK7nPD+wlLvPkUSlU9oacr6og5+Ahh7sut6gzjc2xLhfiK7jOBThpLvoqU4yXeRCPIQ4lHecSOcxTFdEWVSUB1xOF4elopd2Go/V0GO+Rb8atleU 5rgo37HfA+NqmvHvf7bXzfVg3dTNoMmFN0eTlWydfkvPHTKwfNyviuE4+OBqnQrqI5NNkN1tKutDJGvqyJeDmhtmiwgyTF42nHdLqUuoWgkRt5yoV9SzzA76yZUnVZsG7L BmfIfYRsK8/kJiqC9DjBJzw0FsVSVC6+j2BRzmPLEN5RbJGBIIAqlGJVf2fW9oaHSKl40opnxMZVyIrPx/p5K24OPoH34ZcKPzYM5Y/XmBhjaPFoasziUqMoWZGpbYsdMA kNk0rpu9PiMPHRO0inj/gVRLCvoAJmG/f//R9RIkk3UfvZ2HLqnI0F4qLvW54IMFNsZULf3jBUbHoTKl2dTWQgNjyIpgkjAuoVKnCNLMa9HyWrl62bEgVDmqhOMPLT+BHN Vx9z8TrsPJ5dLY9bQcz4qtGonIkgTF2i7XeRYRdRB2QWYf2utAlodJv7KBT34KvVQcCioDxNrzjd4wFuOIia0aygZ+1xY3WnyK5gp1+mGQ2DmzIwK9wAeskMGjLUqz5e0M ZBGokDGfmosXg=

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):	4.34073093788447
Encrypted:	false
SSDEEP:	12288:56rBKJXpdZJJUnu54Rb0Apulwtiu3jSbKsy3JLMmQtse6T3MsDN2U:ErBKJXpdZJJUnu5tmZ
MD5:	77E11E4149B7FE6CEC19BF459E6C137C
SHA1:	F7D31EDABDDA61F55D4AD95AED589103334ECB0E
SHA-256:	FA6471295372FD6E5CE8085FE30329FF45AA6CB77AA24B341CC7052D14322CB9
SHA-512:	C4ACACAE5319A29C1C7BC459FF759306D50F8B19EF597991AD98877693B258E10BCF4F869A2C7BD2170787162D47E54A82752E580D3CAFD37AE2A4E11CC01E 0
Malicious:	false
Reputation:	unknown
Preview:	regfY...Y...p.\.,..... ....P.....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.n..... ....(gQ..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.814516701571545
Encrypted:	false
SSDEEP:	192:QIPuf1VvbyMA9YN5FSE9xMMX9qVWnxCSl4mUhJ9J0wA5LaGCuJT:rGZ5NX9nxJl4nhfu5LtZN
MD5:	DE2D1F6959E729BB32B0E0EB511AC77B
SHA1:	5551C64A82B9BD7A48D800719180061CF0C1FFF8
SHA-256:	8B3F9EA2F18C9021561B7D33812890A335926258654B4A22DC2DB1D8FB20807B
SHA-512:	C9916C5F83D25FE5BFD882CA3A9A6552CF1AECD8036D95CD1AE1B7391ED3A7ACD0EBD80F6E510F6D70A48AC516D30F45F696F801DDC1564AEA812837121FC F5
Malicious:	false
Reputation:	unknown
Preview:	regfX...X...p.\.,..... ....P.....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.n..... ....(gQHvLE.>.....X....P.....].-G|7..>/.9..`.....@.....hbin.....p.\.,.....nk,. .p.....h..... .....&...{ad79c032-a2ea-f756-e377-7 2fb9332c3ae}.....nk . .p..... .....P..... .....Z.....Root.....lf.....Root....nk . .p.....}..... .....*.....DeviceCensus..... ...vk.....WritePermissionsCheck.....p...

C:\Windows\appcompat\Programs\Amcache.hve.tmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.8877681840562437
Encrypted:	false
SSDEEP:	48:9oHVMGzfwYdAXUm/3SS3eX5/cwlApldplCPjD04zISwu:9oRzfw1VfC0QALdLq/zIDu
MD5:	E19D07256C4146E6F0A4F62A28C5923F
SHA1:	72608DED5038D34975296BCC3A9D2FDB9A299FB8

SHA-256:	4C456602AFD47C6C34CCFE490DD32273B14F8BF95337A7EAB39466E1CEF09E31
SHA-512:	69519A46DAC9BD5D6C05C769568BF50B25A75AEBAD2FE204FF371D2684C42EBFC66FA828A172456E2366600A01A4843C4294F6CCC0F666176F307B062F3AFC2
Malicious:	false
Reputation:	unknown
Preview:	regf..... .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...t.m.p....-.....W...-.....W.....-.....W..rmtm".p..... .....I..... .....

C:\Windows\appcompat\Programs\Amcache.hve.tmp.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.9212743368190985
Encrypted:	false
SSDEEP:	48:NuHVMGnVfwYdAXUm/3SS3eX5/cwlApldplCPjD04zISwu:NuRnVfw1VfC0QALdLq/zIDu
MD5:	543F8F4BDB57CCC30BBB25454C338DDA
SHA1:	EABF1601B6AFB905F1E9886F4B4DF695052D83F7
SHA-256:	E4A480EBD169752742691437C0578CD5B57E1B2E658366E44752DB0DFD2C5E23
SHA-512:	ED3F438B254F0F1EE78D1CED5B24F04D42B6FFAC9C132236D906BB59C4392FB82925320CB37D4880112084479E25750C276144221536F4BC8BE8F9BAA18F717F
Malicious:	false
Reputation:	unknown
Preview:	regf..... .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...t.m.p....-.....W...-.....W.....-.....W..rmtm".p..... .....O...HvLE.....\.7..h..R..]'.....hbin..... .p.....nk,. .p.....h.....0.....&...{11517B7C-E79D-4e20-961B-75A 811715ADD}|.....sk.....(.....8.....1.?I.cL<.P...b....~z.....8.....1.?I.cL<.P...b....~z.....?..... .....?.....?..... ... .

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.774709126218966
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	qbot1.dll
File size:	878008
MD5:	682b7633158d20f720ca61cc96c45c50
SHA1:	1f409c817fdf4d65c1f2009f925b583672f67619
SHA256:	83380409b59ca7c171c09f2972034ec5d1789b6e5830e333a897dc4ac1ec885e
SHA512:	3da1b7d9e770217221cf26f8e88af84698b8b2c50a09cba0383d23edce73fecaa2d90715288844d3a3f2bf6d7d8836811982109ffc76ba336deb9029633bb536
SSDEEP:	12288:ovXYcP7kXn89DhAw1aUN3RFEycMFSDXxqEbHXeL/Lt72G3m0ch:mvTkXnyD6ORDccmEs3M/Lt72G3m0
TLSH:	F7156CF25A01867DE2AD117189FDEB5F803E99D04B38A2C3729C5A6A1DB18D31F36713
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.Fz[XFz[XFz[XO..XBz[X]..XCz[XFzZX.x[X.4.XGz[X]..XEz[X]..XKz[X]..X!z[X]..XGz[X]..XGz[X]..XGz[XRichFz[X.....PE..L..

File Icon

Icon Hash:	8e928ba39ed82079

Static PE Info

General

Entrypoint:	0x1005c5fa
Entrypoint Section:	.text
Digitally signed:	true

Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5036D5DC [Fri Aug 24 01:16:12 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ecbfa0c187b811cd9c0664ba6d0c27aa

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

Entrypoint Preview
Instruction
mov eax, 00000001h
retn 000Ch
add dword ptr [ebp+05h], esi
call 00007FA60CE85963h
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007FA60CE85481h
pop ecx
pop ebp
retn 000Ch
int3
jmp dword ptr [1006A090h]
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push 1005C689h
push dword ptr fs:[00000000h]
mov eax, dword ptr [esp+10h]
mov dword ptr [esp+10h], ebp
lea ebp, dword ptr [esp+10h]

Instruction
sub esp, eax
push ebx
push esi
push edi
mov eax, dword ptr [10094144h]
xor dword ptr [ebp-04h], eax
xor eax, ebp
push eax
mov dword ptr [ebp-18h], esp
push dword ptr [ebp-08h]
mov eax, dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFEh
mov dword ptr [ebp-08h], eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
ret
mov ecx, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov edi, edi
push ebp
mov ebp, esp
push dword ptr [ebp+14h]
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
push 1005C09Ah
push 10094144h
call 00007FA60CE85966h
add esp, 18h
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 00000328h
mov dword ptr [10094308h], eax
mov dword ptr [00004304h], ecx

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729 • [IMP] VS2010 SP1 build 40219 • [ASM] VS2010 SP1 build 40219 • [C] VS2010 SP1 build 40219 • [C++] VS2010 SP1 build 40219 • [EXP] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [LNK] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x8cc20	0x4480	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x85be4	0x64	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x95000	0xa18	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xa0000	0x1c90	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x96000	0xca3c	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6aa30	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x73c48	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x6a000	0xa14	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x68745	0x68800	False	0.3936271119916268	data	6.339556700724658	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x6a000	0x270a0	0x27200	False	0.3806784145367412	data	5.524617438010386	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x92000	0x2544	0x2200	False	0.34627757352941174	data	5.345647866062178	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x95000	0x2b508	0x2c000	False	0.8748335404829546	data	7.645313379162503	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc1000	0xd3b2	0xd400	False	0.6316701061320755	data	6.608874822602809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x95140	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_GROUP_ICON	0x95428	0x14	data	English	United States
RT_VERSION	0x9543c	0x480	data	English	United States
RT_MANIFEST	0x958bc	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetCurrentThreadId, GetTickCount, QueryPerformanceCounter, DisableThreadLibraryCalls, IsProcessorFeaturePresent, IsDebuggerPresent, SetUnhandledExceptionFilter, UnhandledExceptionFilter, TerminateProcess, InterlockedCompareExchange, Sleep, InterlockedExchange, DecodePointer, EncodePointer, GetModuleHandleA, GetProcAddress, GetVersionExA, GetSystemInfo, GetCurrentProcess, GetCurrentProcessId, GetSystemTimeAsFileTime
USER32.dll	GetMonitorInfoA, GetWindowThreadProcessId, SetForegroundWindow, EnumDisplayMonitors

Exports

Name	Ordinal	Address
m?0API@ScScript@@IAE@AAVEngine@1@H@Z	1	0x10001610
m?0BinaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@1@Z	2	0x10037fd0
m?0BreakpointInfo@ScScript@@QAE@ABV01@@Z	3	0x100251c0
m?0BreakpointInfo@ScScript@@QAE@XZ	4	0x10025150
m?0Callback@ScScript@@QAE@XZ	5	0x10001330
m?0DataPool@ScScript@@QAE@XZ	6	0x10004cc0
m?0DebugAPI@ScScript@@AAE@AAVEngine@1@@Z	7	0x10025ee0
m?0Debugger@ScScript@@QAE@ABV01@@Z	8	0x10001460
m?0Debugger@ScScript@@QAE@XZ	9	0x10004eb0

Name	Ordinal	Address
m?0Dispatcher@ScScript@@QAE@PBD@Z	10	0x10007260
m?0ESContext@ScScript@@IAE@XZ	11	0x10009d80
m?0EmptyNode@ScScript@@QAE@ABUScanInfo@1@@Z	12	0x10037f00
m?0Engine@ScScript@@IAE@XZ	13	0x100094f0
m?0FileDisp@ScScript@@QAE@XZ	14	0x10024110
m?0GlobalDialogs@ScScript@@QAE@XZ	15	0x1002a3f0
m?0HiliteAPI@ScScript@@AAE@AAVEngine@1@@Z	16	0x1002a080
m?0LabelNode@ScScript@@QAE@ABUScanInfo@1@@Z	17	0x10038270
m?0ListNode@ScScript@@QAE@ABUScanInfo@1@@Z	18	0x10038140
m?0LiveObjectAPI@ScScript@@AAE@AAVEngine@1@@Z	19	0x1002a690
m?0Node@ScScript@@QAE@ABUScanInfo@1@@Z	20	0x10037280
m?0ParserAPI@ScScript@@AAE@AAVEngine@1@@Z	21	0x1002a840
m?0Preprocessor@ScScript@@QAE@XZ	22	0x100104f0
m?0ProfilerData@ScScript@@QAE@XZ	23	0x10001710
m?0RuntimeError@ScScript@@QAE@ABV01@@Z	24	0x10008e10
m?0RuntimeError@ScScript@@QAE@XZ	25	0x10008d20
m?0ScopeInfo@ScScript@@QAE@XZ	26	0x10019230
m?0ScopeNode@ScScript@@QAE@ABUScanInfo@1@@Z	27	0x10038360
m?0Script@ScScript@@QAE@XZ	28	0x10001590
m?0ScriptContainer@ScScript@@QAE@XZ	29	0x100194a0
m?0ScriptContainer@ScScript@@QAE@_N@Z	30	0x10019520
m?0TernaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@11@Z	31	0x10038080
m?0UnaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@@Z	32	0x10037f30
m?0ValidateData@ScScript@@QAE@ABV01@@Z	33	0x10055dd0
m?0ValidateData@ScScript@@QAE@XZ	34	0x10055dc0
m?1API@ScScript@@UAE@XZ	35	0x10001660
m?1BinaryNode@ScScript@@UAE@XZ	36	0x10038000
m?1BreakpointInfo@ScScript@@UAE@XZ	37	0x10025290
m?1Callback@ScScript@@UAE@XZ	38	0x10001660
m?1DataPool@ScScript@@QAE@XZ	39	0x10003dc0
m?1DebugAPI@ScScript@@UAE@XZ	40	0x10001660
m?1Debugger@ScScript@@UAE@XZ	41	0x10004ed0
m?1Dispatcher@ScScript@@UAE@XZ	42	0x10007e00
m?1ESContext@ScScript@@MAE@XZ	43	0x10009e90
m?1EmptyNode@ScScript@@UAE@XZ	44	0x100017e0
m?1Engine@ScScript@@UAE@XZ	45	0x100095a0
m?1FileDisp@ScScript@@UAE@XZ	46	0x100241d0
m?1GlobalDialogs@ScScript@@UAE@XZ	47	0x10001770
m?1HiliteAPI@ScScript@@UAE@XZ	48	0x10001660
m?1LabelNode@ScScript@@UAE@XZ	49	0x100382f0
m?1ListNode@ScScript@@UAE@XZ	50	0x100381d0
m?1LiveObjectAPI@ScScript@@UAE@XZ	51	0x10001660
m?1Node@ScScript@@UAE@XZ	52	0x10037e90
m?1ParserAPI@ScScript@@UAE@XZ	53	0x10001660
m?1Preprocessor@ScScript@@UAE@XZ	54	0x10010cb0
m?1RuntimeError@ScScript@@UAE@XZ	55	0x10008da0
m?1ScopeInfo@ScScript@@UAE@XZ	56	0x100192c0
m?1ScopeNode@ScScript@@UAE@XZ	57	0x10038400
m?1Script@ScScript@@MAE@XZ	58	0x10008d10
m?1ScriptContainer@ScScript@@UAE@XZ	59	0x10019ce0
m?1TernaryNode@ScScript@@UAE@XZ	60	0x100380b0
m?1UnaryNode@ScScript@@UAE@XZ	61	0x10037f60
m?1ValidateData@ScScript@@UAE@XZ	62	0x10055e50
m?4BreakpointInfo@ScScript@@QAEAAV01@ABV01@@Z	63	0x10025240
m?4Debugger@ScScript@@QAEAAV01@ABV01@@Z	64	0x10001490
m?4InitTerm@ScScript@@QAEAAV01@ABV01@@Z	65	0x100016e0
m?4RuntimeError@ScScript@@QAEAAV01@ABV01@@Z	66	0x10008eb0
m?4ValidateData@ScScript@@QAEAAV01@ABV01@@Z	67	0x100016e0
m?_7API@ScScript@@6B@	68	0x1006aac0

Name	Ordinal	Address
m?_7BinaryNode@ScScript@@6B@	69	0x100704dc
m?_7BreakpointInfo@ScScript@@6B@	70	0x1006e89c
m?_7Callback@ScScript@@6B@	71	0x1006aa50
m?_7DebugAPI@ScScript@@6B@	72	0x1006e940
m?_7Debugger@ScScript@@6B@	73	0x1006aa7c
m?_7Dispatcher@ScScript@@6B@	74	0x1006c41c
m?_7ESContext@ScScript@@6B@	75	0x1006c60c
m?_7EmptyNode@ScScript@@6B@	76	0x10070484
m?_7Engine@ScScript@@6B@	77	0x1006c53c
m?_7FileDisp@ScScript@@6B@	78	0x1006e79c
m?_7GlobalDialogs@ScScript@@6B@	79	0x1006ec04
m?_7HiliteAPI@ScScript@@6B@	80	0x1006eb58
m?_7LabelNode@ScScript@@6B@	81	0x10070560
m?_7ListNode@ScScript@@6B@	82	0x10070534
m?_7LiveObjectAPI@ScScript@@6B@	83	0x1006ec6c
m?_7Node@ScScript@@6B@	84	0x1007044c
m?_7ParserAPI@ScScript@@6B@	85	0x1006ec74
m?_7Preprocessor@ScScript@@6B@	86	0x1006ca10
m?_7RuntimeError@ScScript@@6B@	87	0x1006c52c
m?_7ScopeInfo@ScScript@@6B@	88	0x1006cd9c
m?_7ScopeNode@ScScript@@6B@	89	0x1007058c
m?_7Script@ScScript@@6B@	90	0x1006aa9c
m?_7ScriptContainer@ScScript@@6B@	91	0x1006cda4
m?_7TernaryNode@ScScript@@6B@	92	0x10070508
m?_7UnaryNode@ScScript@@6B@	93	0x100704b0
m?_7ValidateData@ScScript@@6B@	94	0x10072178
m?_FDispatcher@ScScript@@QAEXXZ	95	0x10001580
m_isInteger@DataPool@ScScript@@ABE_NH@Z	96	0x10004380
m_isUInteger@DataPool@ScScript@@ABE_NH@Z	97	0x100044e0
madd@DataPool@ScScript@@QAEHABVVariant@ScCore@@@Z	98	0x10004140
madd@DataPool@ScScript@@QAEHG@Z	99	0x100013d0
madd@DataPool@ScScript@@QAEHI@Z	100	0x10004070
madd@DataPool@ScScript@@QAEHN@Z	101	0x10003fc0
madd@DataPool@ScScript@@QAEHPBD@Z	102	0x10003de0
madd@DataPool@ScScript@@QAEHPBG@Z	103	0x10003ee0
madd@ScriptContainer@ScScript@@QAEXABV12@_N@Z	104	0x100197a0
maddClass@Dispatcher@ScScript@@QAEXABVString@ScCore@@@Z	105	0x10007390
maddClass@Dispatcher@ScScript@@QAEXPBD@Z	106	0x10007f30
maddProperties@Dispatcher@ScScript@@QAEXHPBUPropEntry@2@PBD@Z	107	0x10001530
matExit@InitTerm@ScScript@@SAXP6AXXZ@Z	108	0x1000a820
mcall@Dispatcher@ScScript@@QAEXAAUArguments@2@PBD@Z	109	0x10007990
mcall@Dispatcher@ScScript@@UAEXAAUArguments@2@P6AX0@Z@Z	110	0x10006b20
mcall@GlobalDialogs@ScScript@@UAEHAAVLiveObject@ScCore@@HABVArray@4@AAVVariant@4@PAVError@4@@Z	111	0x1002a470
mcheckStack@ESContext@ScScript@@QBE_NXZ	112	0x10001810
mclearError@Engine@ScScript@@UAEXXZ	113	0x10009170
mclone@Engine@ScScript@@UBEHPAPAV12@@Z	114	0x10009650
mcommand@DebugAPI@ScScript@@QAEXW4Cmd@12@_N@Z	115	0x10026050
mcompile@ScriptContainer@ScScript@@QAEHABVFileSpec@ScCore@@_NP6A_N0@Z@Z	116	0x1001a140
mcompile@ScriptContainer@ScScript@@QAEHABVString@ScCore@@0@Z	117	0x10019610
mcreateEngine@Engine@ScScript@@SAPAV12@W4Type@12@@Z	118	0x10008fe0
mcreateFile@FileDisp@ScScript@@QAE_NAAVVariant@ScCore@@ABVString@4@@Z	119	0x100242a0
mcreateFolder@FileDisp@ScScript@@QAE_NAAVVariant@ScCore@@ABVString@4@@Z	120	0x100241e0
mcreateValidateVTable@ValidateData@ScScript@@SAPAVHashTable@ScCore@@XZ	121	0x10055de0
mdebugBreak@DebugAPI@ScScript@@QBEXABVString@ScCore@@@Z	122	0x10025f70
mdecRef@ScopeInfo@ScScript@@QBEXXZ	123	0x10001700
mdecompile@ParserAPI@ScScript@@QBE?AVString@ScCore@@ABVScopeNode@2@@Z	124	0x1002a810
mdirective@Preprocessor@ScScript@@AAE_NAAUProcData@12@@Z	125	0x10010570
mdoProcess@Preprocessor@ScScript@@AAE_NAAUProcData@12@@Z	126	0x10010040

Name	Ordinal	Address
mdump@BinaryNode@ScScript@@UAEXAAVEngine@2@H@Z	127	0x10037e40
mdump@LabelNode@ScScript@@UAEXAAVEngine@2@H@Z	128	0x10037e70
mdump@ListNode@ScScript@@UAEXAAVEngine@2@H@Z	129	0x10037e60
mdump@Node@ScScript@@UAEXAAVEngine@2@H@Z	130	0x10037e20
mdump@ScopeNode@ScScript@@UAEXAAVEngine@2@H@Z	131	0x10037e80
mdump@TernaryNode@ScScript@@UAEXAAVEngine@2@H@Z	132	0x10037e50
mdump@UnaryNode@ScScript@@UAEXAAVEngine@2@H@Z	133	0x10037e30
menablePreProcessor@ParserAPI@ScScript@@QAE_N_N@Z	134	0x1002a770
mengineNotify@Callback@ScScript@@UAEXAAVEngine@2@HH@Z	135	0x10001950
menterDebugMode@Callback@ScScript@@UAEXAAVEngine@2@@Z	136	0x100018f0
merase@ScriptContainer@ScScript@@QAEXXZ	137	0x10019820
merrorAlert@ScriptContainer@ScScript@@QBEXXZ	138	0x1001a0c0
merrorAlert@ScriptContainer@ScScript@@SAXABVError@ScCore@@@Z	139	0x1001a040
merrorMessage@ScriptContainer@ScScript@@QBE?AVString@ScCore@@XZ	140	0x10019d60
merrorMessage@ScriptContainer@ScScript@@SA?AVString@ScCore@@ABVError@4@@Z	141	0x10019870
meval@DebugAPI@ScScript@@QAEHABVString@ScCore@@AAVVariant@4@@Z	142	0x100261c0
mexecute@ScriptContainer@ScScript@@QAEHAAVEngine@2@H@Z	143	0x10019f90
mexecuteStaticXML@DebugAPI@ScScript@@SAPAVXML@ScCore@@ABV34@AAVError@4@@Z	144	0x10029d00
mexecuteXML@DebugAPI@ScScript@@QAEPAVXML@ScCore@@ABV34@AAVError@4@@Z	145	0x100298b0
mexit@InitTerm@ScScript@@SAXXZ	146	0x1000a840
mfindEngine@Engine@ScScript@@SAPAV12@ABVString@ScCore@@@Z	147	0x10009360
mfindProperty@Dispatcher@ScScript@@UBEPBVPropInfo@2@HHPAVRoot@ScCore@@_N1@Z	148	0x10007790
mfoldConstants@BinaryNode@ScScript@@UAEPAVNode@2@XZ	149	0x10038680
mfoldConstants@ListNode@ScScript@@UAEPAVNode@2@XZ	150	0x10038c90
mfoldConstants@Node@ScScript@@UAEPAV12@XZ	151	0x100373e0
mfoldConstants@TernaryNode@ScScript@@UAEPAVNode@2@XZ	152	0x10038c30
mfoldConstants@UnaryNode@ScScript@@UAEPAVNode@2@XZ	153	0x10038480
mgarbageCollecting@Callback@ScScript@@UAE_NAAVEngine@2@@Z	154	0x100018d0
mgcAll@Engine@ScScript@@SAXXZ	155	0x100093e0
mget@DataPool@ScScript@@SAAAV12@XZ	156	0x10003c00
mget@Dispatcher@ScScript@@UAEXAAUArguments@2@@Z	157	0x10006ae0
mget@ESContext@ScScript@@SAAAV12@XZ	158	0x10009e50
mgetAll@Engine@ScScript@@SAXAAV?$TSimpleArray@VEngine@ScScript@@@ScCore@@@Z	159	0x100093c0
mgetBreakpoints@DebugAPI@ScScript@@QBEXAAV?$TSimpleArray@VBreakpointInfo@ScScript@@@ScCore@@@Z	160	0x100254d0
mgetCallback@Engine@ScScript@@QBEPAVCallback@2@XZ	161	0x10009120
mgetClass@Dispatcher@ScScript@@QBEABVString@ScCore@@H@Z	162	0x100074b0
mgetClassCount@Dispatcher@ScScript@@QBEHXZ	163	0x10006a50
mgetClassID@Dispatcher@ScScript@@ABEHH@Z	164	0x10006a60
mgetClassInfo@Dispatcher@ScScript@@UAEPBVClassInfo@ScCore@@ABVString@4@@Z	165	0x10006b40
mgetClassObject@Callback@ScScript@@UAEPAVLiveObject@ScCore@@AAVEngine@2@ABVString@4@AAI@Z	166	0x10001920
mgetConstant@Node@ScScript@@QBEPBVVariant@ScCore@@XZ	167	0x10001640
mgetContextInfo@DebugAPI@ScScript@@QBEHHAAVString@ScCore@@AAVArray@4@@Z	168	0x10026430
mgetContextLevel@DebugAPI@ScScript@@QBEHXZ	169	0x10001760
mgetCurrent@Engine@ScScript@@SAPAV12@XZ	170	0x10008fd0
mgetDebugFlags@Engine@ScScript@@QBEHXZ	171	0x100016b0
mgetDebugLevel@Engine@ScScript@@QBEHXZ	172	0x10001690
mgetDebugState@DebugAPI@ScScript@@QBE?AW4State@12@XZ	173	0x10025f20
mgetDictionary@Engine@ScScript@@UBEPAVDictionary@ScCore@@XZ	174	0x10009100
mgetDirective@Preprocessor@ScScript@@QBEPBVString@ScCore@@ABV34@@Z	175	0x10010a90
mgetEngine@API@ScScript@@QBEAAVEngine@2@XZ	176	0x10001650
mgetEnumNames@Dispatcher@ScScript@@UBEXABVVariant@ScCore@@AAV?$TSimpleArray@VString@ScCore@@@4@@Z	177	0x10006ad0
mgetEnumerableProperties@Dispatcher@ScScript@@UBEXABVVariant@ScCore@@AAVSimpleArray@4@H@Z	178	0x100080e0
mgetError@Engine@ScScript@@UBEABVError@ScCore@@XZ	179	0x10009160
mgetError@ScriptContainer@ScScript@@QBEAAVError@ScCore@@XZ	180	0x100195c0

Name	Ordinal	Address
mgetErrorInfo@Engine@ScScript@@UBEABVRuntimeError@2@XZ	181	0x10009140
mgetGlobalObject@LiveObjectAPI@ScScript@@QBEAAVLiveObject@ScCore@@XZ	182	0x1002a390
mgetID@Engine@ScScript@@QBEIXZ	183	0x10009050
mgetIncludePath@ParserAPI@ScScript@@QBEABVString@ScCore@@XZ	184	0x1002a790
mgetIncludes@Preprocessor@ScScript@@QBEABVString@ScCore@@XZ	185	0x10010460
mgetInteger@DataPool@ScScript@@QBEHH@Z	186	0x10004b30
mgetLocalizer@Engine@ScScript@@QBEPBVLocalizer@ScCore@@XZ	187	0x100090e0
mgetName@API@ScScript@@QBEHXZ	188	0x10001640
mgetName@Engine@ScScript@@QBEABVString@ScCore@@XZ	189	0x10009060
mgetNode@ListNode@ScScript@@QBEPAVNode@2@H@Z	190	0x10001870
mgetNumber@DataPool@ScScript@@QBENH@Z	191	0x10004640
mgetOutputStream@DebugAPI@ScScript@@QBEPAVFile@ScCore@@XZ	192	0x10001750
mgetParent@Dispatcher@ScScript@@QBEPAV12@XZ	193	0x100069e0
mgetProfilerData@DebugAPI@ScScript@@QAEXPAV? $TSimpleArray@VProfilerData@ScScript@@@ScCore@@_N@Z	194	0x100265f0
mgetProfilingLevel@Engine@ScScript@@QBEHXZ	195	0x100016a0
mgetProperties@DebugAPI@ScScript@@QAE_NABVVariant@ScCore@@AAV? $THashTable@VVariant@ScCore@@@4@H@Z	196	0x10026750
mgetProperties@DebugAPI@ScScript@@QAE_NABVVariant@ScCore@@AAV? $THashTable@VVariant@ScCore@@@4@_N2@Z	197	0x10029e80
mgetProperties@Dispatcher@ScScript@@UBEXHHAAV? $TSimpleArray@$$CBVPropInfo@ScScript@@@ScCore@@@Z	198	0x10007600
mgetPropertyTable@GlobalDialogs@ScScript@@SAABULivePropertyInfo@ScCore@@XZ	199	0x1002a460
mgetScript@DebugAPI@ScScript@@QBEPAVScript@2@XZ	200	0x10026220
mgetScript@ScriptContainer@ScScript@@QBEPAVScript@2@H@Z	201	0x100195d0
mgetSecurityFlags@FileDisp@ScScript@@QBEHXZ	202	0x10001750
mgetSource@DebugAPI@ScScript@@QBE?AVString@ScCore@@XZ	203	0x10026270
mgetSourceFileID@DebugAPI@ScScript@@QBEHXZ	204	0x10026310
mgetSourceLine@DebugAPI@ScScript@@QBEHXZ	205	0x10026340
mgetStackDepth@DebugAPI@ScScript@@QBEHXZ	206	0x10026480
mgetStackTrace@DebugAPI@ScScript@@QBE?AVString@ScCore@@HH@Z	207	0x10026370
mgetSymbol@DataPool@ScScript@@QBE?AVString@ScCore@@H@Z	208	0x100049e0
mgetTable@Dispatcher@ScScript@@ABEPBVTableEntry@2@H@Z	209	0x100074f0
mgetUInteger@DataPool@ScScript@@QBEIH@Z	210	0x10004bd0
mgetUserData@Dispatcher@ScScript@@QBEPAVRoot@ScCore@@XZ	211	0x10001550
mgetUserData@Engine@ScScript@@QBEPAVRoot@ScCore@@XZ	212	0x10001550
mgetValue@DataPool@ScScript@@QBEXHAAVVariant@ScCore@@@Z	213	0x10004790
mgetVersion@Engine@ScScript@@SAHXZ	214	0x10008fc0
mgetWatchpointInfo@DebugAPI@ScScript@@QAE_NAAVVariant@ScCore@@00@Z	215	0x100254f0
mgetXML@LiveObjectAPI@ScScript@@QBEPAVXML@ScCore@@ABVVariant@4@@Z	216	0x1002a3b0
mhasDotProperties@Dispatcher@ScScript@@QBE_NH@Z	217	0x10007570
mhasOperators@Dispatcher@ScScript@@ABE_NH@Z	218	0x100075c0
mhasProperty@Dispatcher@ScScript@@UBEPBUPropEntry@2@ABVVariant@ScCore@@0_N@Z	219	0x10006ac0
mincRef@ScopeInfo@ScScript@@QBEXXZ	220	0x100016f0
minit@InitTerm@ScScript@@SAXXZ	221	0x1000a6e0
minit@ValidateData@ScScript@@SAXXZ	222	0x10055ed0
minsert@ScriptContainer@ScScript@@QAEXAAVScript@2@H@Z	223	0x10019740
minvalidateClassAll@Engine@ScScript@@SAXABVString@ScCore@@@Z	224	0x100094a0
misClass@Dispatcher@ScScript@@QBE_NABVString@ScCore@@@Z	225	0x100069f0
misClass@Dispatcher@ScScript@@QBE_NH@Z	226	0x10006a30
misClass@Dispatcher@ScScript@@QBE_NPBD@Z	227	0x10007440
misCommandEnabled@DebugAPI@ScScript@@QAE_NW4Cmd@12@@Z	228	0x10025f90
misContinueOnError@ScriptContainer@ScScript@@QBE_NXZ	229	0x100195a0
misEmpty@Node@ScScript@@QBE_NXZ	230	0x100017d0
misInitialized@InitTerm@ScScript@@SA_NXZ	231	0x1000a800
misInteger@DataPool@ScScript@@QBE_NH@Z	232	0x100013e0
misNumber@DataPool@ScScript@@QBE_NH@Z	233	0x10004210
misReadOnly@DebugAPI@ScScript@@QAE_NABVVariant@ScCore@@ABVString@4@@Z	234	0x10026ac0
misUInteger@DataPool@ScScript@@QBE_NH@Z	235	0x10001420
misUpperCase@DataPool@ScScript@@SA_NH@Z	236	0x100013b0

Name	Ordinal	Address
misValidClassName@Callback@ScScript@@UAE_NAAVEngine@2@ABVString@ScCore@@@Z	237	0x10001940
misValidLine@Script@ScScript@@SA_NABV12@H@Z	238	0x10045560
mleaveDebugMode@Callback@ScScript@@UAEXAAVEngine@2@_N@Z	239	0x10001900
mlength@ListNode@ScScript@@QBEHXZ	240	0x100017f0
mlength@ScriptContainer@ScScript@@QBEJXZ	241	0x100195b0
mload@ScriptContainer@ScScript@@QAEHAAVEngine@2@@Z	242	0x100196a0
mlockRef@Engine@ScScript@@QAEXABVVariant@ScCore@@@Z	243	0x100016d0
mmakeXMLObject@LiveObjectAPI@ScScript@@QBEXABVXML@ScCore@@AAVVariant@4@@Z	244	0x1002a3d0
mnext@HiliteAPI@ScScript@@QAE_NPAVHiliteAPIData@2@AAUHiliteRange@2@@Z	245	0x1002a0b0
mparse@ParserAPI@ScScript@@QBEPAVScopeNode@2@ABVString@ScCore@@@Z	246	0x1002a870
mprocess@Preprocessor@ScScript@@QAEHABVString@ScCore@@0AAV34@PAVError@4@@Z	247	0x10010b20
mput@Dispatcher@ScScript@@UAEXAAUArguments@2@@Z	248	0x10006b00
mregisterProperties@Dispatcher@ScScript@@QAEXHPBUPropEntry@2@@Z	249	0x100083e0
mregisterProperties@Dispatcher@ScScript@@QAEXHPBUPropEntry@2@ABVString@ScCore@@@Z	250	0x10007fa0
mregisterProperties@Dispatcher@ScScript@@QAEXHPBUPropEntry@2@PBD@Z	251	0x10008420
mrestoreError@Engine@ScScript@@UAEXABVError@ScCore@@@Z	252	0x10009180
mrunning@Callback@ScScript@@UAEXAAVEngine@2@@Z	253	0x100018c0
mruntimeError@Callback@ScScript@@UAEXAAVEngine@2@@Z	254	0x100018e0
mset@RuntimeError@ScScript@@QAEXABVError@ScCore@@@Z	255	0x10008f10
msetBreakpoints@DebugAPI@ScScript@@QAEXPBV?$TSimpleArray@VBreakpointInfo@ScScript@@@ScCore@@@Z	256	0x100254e0
msetCallback@Engine@ScScript@@QAEXPAVCallback@2@@Z	257	0x10009130
msetContextLevel@DebugAPI@ScScript@@QAEXH@Z	258	0x100254b0
msetDebugFlags@Engine@ScScript@@QAEXH@Z	259	0x100016c0
msetDebugLevel@Engine@ScScript@@QAEXH@Z	260	0x10009070
msetDictionary@Engine@ScScript@@UAEXPAVDictionary@ScCore@@@Z	261	0x10009110
msetError@Engine@ScScript@@UAEXABVError@ScCore@@@Z	262	0x10009890
msetError@Engine@ScScript@@UAEXABVRuntimeError@2@@Z	263	0x10009b10
msetError@Engine@ScScript@@UAEXH@Z	264	0x10009190
msetError@Engine@ScScript@@UAEXHABVLiveObject@ScCore@@H_NH@Z	265	0x10009200
msetError@Engine@ScScript@@UAEXHABVString@ScCore@@H_N@Z	266	0x100099f0
msetGlobalObject@LiveObjectAPI@ScScript@@QBEXAAVLiveObject@ScCore@@@Z	267	0x1002a3a0
msetIncludePath@ParserAPI@ScScript@@QBEXABVString@ScCore@@@Z	268	0x1002a7a0
msetIncludes@Preprocessor@ScScript@@QAEXABVString@ScCore@@@Z	269	0x10010470
msetLocalizer@Engine@ScScript@@QAEXPBVLocalizer@ScCore@@@Z	270	0x100090f0
msetName@Engine@ScScript@@QAE_NABVString@ScCore@@@Z	271	0x100096b0
msetOutputStream@DebugAPI@ScScript@@QAEXPAVFile@ScCore@@@Z	272	0x10001740
msetProfilingLevel@Engine@ScScript@@QAEXH@Z	273	0x100090b0
msetSecurityFlags@FileDisp@ScScript@@QAEXH@Z	274	0x10001740
msetStackBottom@ESContext@ScScript@@QAEXH@Z	275	0x10001800
msetUserData@Dispatcher@ScScript@@QAEXPAVRoot@ScCore@@_N@Z	276	0x10001560
msetUserData@Engine@ScScript@@QAEXPAVRoot@ScCore@@_N@Z	277	0x10001670
mstart@HiliteAPI@ScScript@@QAEPAVHiliteAPIData@2@ABVString@ScCore@@HH@Z	278	0x10029f70
mstop@HiliteAPI@ScScript@@QAEXPAVHiliteAPIData@2@@Z	279	0x1002a050
msubClass@Dispatcher@ScScript@@QAEXAAV12@@Z	280	0x10006aa0
mtest_1@ValidateData@ScScript@@UAEXXZ	281	0x10055e60
mtest_2@ValidateData@ScScript@@UAEXXZ	282	0x10055e70
mtest_3@ValidateData@ScScript@@UAEXXZ	283	0x10055e80
mthrowException@ValidateData@ScScript@@SAXXZ	284	0x10055e90
mtoBinaryNode@BinaryNode@ScScript@@UBEPBV12@XZ	285	0x10037460
mtoBinaryNode@Node@ScScript@@UBEPBVBinaryNode@2@XZ	286	0x10037400
mtoLabelNode@LabelNode@ScScript@@UBEPBV12@XZ	287	0x10037490
mtoLabelNode@Node@ScScript@@UBEPBVLabelNode@2@XZ	288	0x10037430
mtoListNode@ListNode@ScScript@@UBEPBV12@XZ	289	0x10037480
mtoListNode@Node@ScScript@@UBEPBVListNode@2@XZ	290	0x10037420
mtoScopeNode@Node@ScScript@@UBEPBVScopeNode@2@XZ	291	0x10037440
mtoScopeNode@ScopeNode@ScScript@@UBEPBV12@XZ	292	0x100374a0

Name	Ordinal	Address
mtoString@BinaryNode@ScScript@@UBE?AVString@ScCore@@XZ	293	0x10037960
mtoString@LabelNode@ScScript@@UBE?AVString@ScCore@@XZ	294	0x10037b50
mtoString@ListNode@ScScript@@UBE?AVString@ScCore@@XZ	295	0x10038d40
mtoString@Node@ScScript@@UBE?AVString@ScCore@@XZ	296	0x10037700
mtoString@ScopeNode@ScScript@@UBE?AVString@ScCore@@XZ	297	0x10037c50
mtoString@TernaryNode@ScScript@@UBE?AVString@ScCore@@XZ	298	0x10037a40
mtoString@UnaryNode@ScScript@@UBE?AVString@ScCore@@XZ	299	0x100378b0
mtoTernaryNode@Node@ScScript@@UBEPBVTernaryNode@2@XZ	300	0x10037410
mtoTernaryNode@TernaryNode@ScScript@@UBEPBV12@XZ	301	0x10026510
mtoUnaryNode@Node@ScScript@@UBEPBVUnaryNode@2@XZ	302	0x100373f0
mtoUnaryNode@UnaryNode@ScScript@@UBEPBV12@XZ	303	0x10037450
mundefinedError@Callback@ScScript@@UAE_NAAVEngine@2@ABVVariant@ScCore@@1AAV45@@Z	304	0x10001910
munlockRef@Engine@ScScript@@QAEXABVVariant@ScCore@@@Z	305	0x100016d0
next	306	0x10037470

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 1, 2023 21:27:26.990444899 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.032546043 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.032670021 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.033020020 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.075469017 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.081409931 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.084450006 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.645675898 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.686903954 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.687359095 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.687517881 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.688122988 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:27.731060028 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.762924910 CEST	2222	49730	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:27.764712095 CEST	49730	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.492559910 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.534629107 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.535881996 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.536344051 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.597027063 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.597081900 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.597326040 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.599488974 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.602232933 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.602315903 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.648127079 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.648277044 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.653332949 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653367043 CEST	2222	49732	213.64.33.92	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 1, 2023 21:27:42.653379917 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653390884 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653410912 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653431892 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653453112 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653472900 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653491974 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653512955 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.653585911 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.653585911 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.653680086 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.696938992 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.697091103 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.703682899 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703725100 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703749895 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703896046 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703912020 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.703918934 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703942060 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703963995 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703973055 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.703985929 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.703993082 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.704005957 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.704022884 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.704026937 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.704049110 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.704066038 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.704092026 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.738687992 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.738960981 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.746886969 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.747117043 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.751935005 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.751964092 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.751982927 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752187014 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.752381086 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752404928 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752423048 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752441883 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752460003 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752477884 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752496958 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.752505064 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.752541065 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.752588987 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.779994011 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.780792952 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.781001091 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.787924051 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.788029909 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.788773060 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.789233923 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.793484926 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.794975996 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.806771040 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806807995 CEST	2222	49732	213.64.33.92	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 1, 2023 21:27:42.806824923 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806845903 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806865931 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806886911 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806907892 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806967020 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.806988001 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.807009935 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.807032108 CEST	2222	49732	213.64.33.92	192.168.2.5
Jun 1, 2023 21:27:42.807029963 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.807029963 CEST	49732	2222	192.168.2.5	213.64.33.92
Jun 1, 2023 21:27:42.807054996 CEST	2222	49732	213.64.33.92	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 1, 2023 21:27:57.308912039 CEST	192.168.2.5	8.8.8.8	0x1035	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:58.128428936 CEST	192.168.2.5	8.8.8.8	0xf672	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
Jun 1, 2023 21:27:27.272839069 CEST	8.8.8.8	192.168.2.5	0x9a68	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.128	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:27.272839069 CEST	8.8.8.8	192.168.2.5	0x9a68	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		54.161.105.65	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		34.225.127.72	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:57.332308054 CEST	8.8.8.8	192.168.2.5	0x1035	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:58.153315067 CEST	8.8.8.8	192.168.2.5	0xf672	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)	false
Jun 1, 2023 21:27:58.153315067 CEST	8.8.8.8	192.168.2.5	0xf672	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)	false
Jun 1, 2023 21:27:58.153315067 CEST	8.8.8.8	192.168.2.5	0xf672	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- yahoo.com
- www.yahoo.com

Statistics

Behavior

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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **5568**, Parent PID: **3324**

General

Target ID:	0
Start time:	21:23:56
Start date:	01/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\qbot1.dll"
Imagebase:	0xd40000
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: 6356, Parent PID: 5568

General

Target ID:	1
Start time:	21:23:56
Start date:	01/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 6348, Parent PID: 5568

General

Target ID:	2
Start time:	21:23:56
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1
Imagebase:	0x11d0000
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: 6336, Parent PID: 5568

General

Target ID:	3
Start time:	21:23:56
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\qbot1.dll,m?0API@ScScript@@IAE@AAVEngine@1@H@Z
Imagebase:	0x8b0000
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: **6268**, Parent PID: **6348**

General

Target ID:	4
Start time:	21:23:56
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1
Imagebase:	0x8b0000
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: **6648**, Parent PID: **6336**

General

Target ID:	8
Start time:	21:23:57
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6336 -s 656
Imagebase:	0x180000
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	6C0E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E90.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E90.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b96630	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b96630\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E90.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E90.tmp.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E7F.tmp.csv	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6036.tmp.txt	success or wait	1	6C0D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 6e 79 64 fd 05 12 00 00 00 00 00	MDMP nyd	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.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 18 00 00 fd 6e 79 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 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTnyd0=Pacific Standard TimePacific Daylight Time	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.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 10 16 00 10 3c fd 02 fd fd fd fd 10 16 00 10 fd 02 00 02 fd fd 53 00 fd 6b 08 00 23 00 00 00 47 02 01 00 fd fd 53 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++Sk#GS+	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	1620	168	fd 18 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 6b 08 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 6b 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	kk~!	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	10722	20	0a 00 00 00 00 00 74 00 00 00 00 00 fd 04 00 00 fd 2a 00 00	t*	success or wait	10	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	10886	1176	00 00 00 04 fd fd fd 00 00 fd 00 fd 7b 1a 77 58 17 fd 02 00 00 00 00 00 00 fd 02 fd 79 1a 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 2b 76 00 00 00 00 00 00 00 00 00 00 4a 00 00 00 00 00 fd 7b 1a 77 fd fd fd 01 00 00 00 00 00 2c 7f 00 00 00 00 30 07 2c 7f 00 00 3c 7f 28 02 3d 7f 50 06 3e 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 00 03 00 00 00 10 00 00 00 60 66 1a 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 1a 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{wXyw+vJ{w,0,<(=P>m `fwPSwB	success or wait	9	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	22266	5804	fd fd 0f 77 fd 1a fd 74 fd fd fd fd fd fd 53 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wtS$tS	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	9290	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 10 16 00 10 00 00 00 00 fd fd 53 00 fd fd 0f 77 23 00 00 00 02 02 00 00 58 fd 53 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++Sw#XS+	success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	1840	48	fd 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 74 00 00 00 00 00 30 fd fd 00 00 00 00 00 fd 05 00 00 2a 51 00 00 fd 02 00 00 16 27 00 00	`t0*Q'	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	6548	752	00 00 72 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 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 12 fd 03 00 00 00 00 00 5d 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 4d fd 1a 00 00 00 00 00 fd 1b 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 7d 30 05 00 00 00 00	rs0Us@d!BB? #@AZbF]M@}0	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.tmp.dmp	28070	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B33.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 7c 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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6336</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1887</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 32 00 33 00 32 00 32 00 35 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>123232256</PeakVirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 32 00 32 00 34 00 30 00 36 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>123224064</VirtualSize>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 35 00 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>2350</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 30 00 32 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7860224</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 30 00 32 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7860224</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177952</QuotaPeakPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177752</QuotaPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23840</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23568</QuotaNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 31 00 37 00 36 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5017600</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 32 00 35 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5025792</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 31 00 37 00 36 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5017600</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5568</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 36 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2162</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 39 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>893</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 31 00 35 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3215360</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 31 00 37 00 30 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3117056</WorkingSetSize>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>626688</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>634880</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>626688</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4766	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	18	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5550	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5554	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5556	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5596	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5600	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5602	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	6	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	12	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	5648	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6202	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6206	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6208	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6252	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6254	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6300	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6402	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 79 00 62 00 65 00 68 00 6a 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ybehjb, Inc.</SystemManufacturer>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6516	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 79 00 62 00 65 00 68 00 6a 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ybehjb7,1</SystemProductName>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6620	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6748	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 31 00 30 00 38 00 33 00 35 00 38 00 37 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>1641083587</OSInstallDate>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6830	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6834	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6838	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6944	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	6948	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7022	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7068	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7110	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7212	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7254	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7278	4	0d 00 0a 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7282	2	09 00		success or wait	6	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7286	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7536	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7568	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 33 00 3a 00 35 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T04:23:58Z">	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7676	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 32 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 32 00 35 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="365" PID="6336" UptimeMS="125" TimeSinceCreationMS="125" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7942	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7962	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7966	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	7968	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8012	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8058	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 64 00 63 00 32 00 35 00 37 00 30 00 30 00 2d 00 35 00 31 00 65 00 31 00 2d 00 34 00 61 00 35 00 61 00 2d 00 62 00 62 00 35 00 66 00 2d 00 38 00 30 00 64 00 66 00 35 00 64 00 66 00 39 00 33 00 66 00 39 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5dc25700-51e1-4a5a-bb5f-80df5df93f96</Guid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8164	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 33 00 3a 00 35 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T04:23:58Z</CreationTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8268	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E22.tmp.WERInternalMetadata.xml	8312	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E90.tmp.xml	0	4771	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b96630\Report.wer	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b96630\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	172	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b96630\Report.wer	11452	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 38 00 37 00 38 00 32 00 32 00 36 00 30 00 31 00	MetadataHash=1287822601	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\{11517B7C-E79D-4e20-961B-75A811715ADD}	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6C0F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6C0F1FB2	RegCreateKeyExW
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	6C0F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{e9e9cdbe-6ba2-4eaa-94c1-025e96082dd7}	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C0F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6C0F36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 BE 6B 08 00 02 00 00 00 08 00 00 00 BE 6B 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C0F1FE8	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Program Files (x86)\Google\Update\1.3.36.131	\??\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Windows\AppCompat\Programs\Amcache.hve.tmp!\??\C:\Windows\AppCompat\Programs\Amcache.hve	success or wait	1	6C0F36BF	unknown

Analysis Process: WerFault.exe PID: **6644**, Parent PID: **6268**

General

Target ID:	9
Start time:	21:23:57
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6268 -s 660
Imagebase:	0x180000
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	6C0E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F6B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F6B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b56739	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b56739\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F6B.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F6B.tmp.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F7A.tmp.csv	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6131.tmp.txt	success or wait	1	6C0D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 6e 79 64 fd 05 12 00 00 00 00 00	MDMP nyd	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 7c 18 00 00 fd 6e 79 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 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00	UBGenuineIntelWT|nyd0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	8622	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 10 16 00 10 40 fd 5c 03 fd fd fd fd 10 16 00 10 fd 02 00 02 fd fd 27 03 fd 6b 08 00 23 00 00 00 47 02 01 00 fd fd 27 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++@\'k#G'+	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	1620	168	3c 00 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 6b 08 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 6b 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	<kk!	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	11486	20	0d 00 00 00 00 fd 07 03 00 00 00 00 fd 04 00 00 fd 2d 00 00	-	success or wait	13	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	11698	1176	00 00 00 04 fd fd fd 00 00 fd 00 fd 7b 1a 77 fd 17 5c 03 00 00 00 00 00 00 5c 03 fd 79 1a 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 2b 76 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 00 00 fd 7b 1a 77 fd fd fd fd 01 00 00 00 00 00 02 7f 00 00 00 00 30 07 02 7f 00 00 12 7f 28 02 13 7f 50 06 14 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 1a 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 1a 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{w\\yw+v{w0(Pm `fwPSwB	success or wait	12	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	32970	4	14 12 09 77	w	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	9338	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 10 16 00 10 00 00 00 00 fd fd 27 03 fd fd 0f 77 23 00 00 00 12 02 00 00 20 fd 27 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++'w# '+	success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	1888	48	fd 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 08 03 00 00 00 00 fd fd fd 04 00 00 00 00 48 03 00 00 32 7b 00 00 fd 02 00 00 12 2a 00 00	H2{*	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	6596	752	00 00 72 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 b6 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 5d 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 1c 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 7d 30 05 00 00 00 00	rs0Us@!BB?#@AZbF]@}0	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	32974	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C4C.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8TP0	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6268</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2132</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 37 00 35 00 36 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123756544</PeakVirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 37 00 34 00 38 00 33 00 35 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123748352</VirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 35 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2354</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 38 00 38 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7888896</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 38 00 38 00 38 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7888896</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177952</QuotaPeakPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 37 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177752</QuotaPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 34 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>24432</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>24160</QuotaNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5169152</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 37 00 37 00 33 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>5177344</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5169152</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6348</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 35 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2253</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 36 00 32 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57462784</PeakVirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 39 00 37 00 38 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53497856</VirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 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>1110</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 38 00 32 00 31 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>3821568</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 38 00 30 00 39 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3809280</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5768</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5360</QuotaNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 35 00 37 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3571712</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 39 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3579904</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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 35 00 37 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3571712</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4762	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4814	4	0d 00 0a 00		success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4818	2	09 00		success or wait	18	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	4822	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5546	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5550	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5552	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5592	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5596	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5598	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5636	4	0d 00 0a 00		success or wait	6	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5640	2	09 00		success or wait	12	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	5644	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6198	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6202	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6204	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6244	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6248	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6250	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6296	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6390	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6394	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6398	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 79 00 62 00 65 00 68 00 6a 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ybehjb, Inc.</SystemManufacturer>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6512	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 79 00 62 00 65 00 68 00 6a 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ybehjb7,1</SystemProductName>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6608	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6612	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6616	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6736	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6740	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6744	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 31 00 30 00 38 00 33 00 35 00 38 00 37 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>1641083587</OSInstallDate>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6834	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6936	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6940	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	6944	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7012	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7016	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7018	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7058	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7062	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7064	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7106	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7202	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7206	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7208	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7250	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7274	4	0d 00 0a 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7278	2	09 00		success or wait	6	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7282	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7526	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7530	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7532	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7558	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7562	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7564	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 33 00 3a 00 35 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T04:23:58Z">	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7664	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7668	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7672	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 32 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="366" PID="6268" UptimeMS="156" TimeSinceCreationMS="156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7930	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7934	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7938	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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7958	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7962	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	7964	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8002	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8006	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8008	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8054	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 35 00 64 00 38 00 38 00 66 00 34 00 63 00 2d 00 37 00 62 00 34 00 39 00 2d 00 34 00 38 00 65 00 30 00 2d 00 61 00 31 00 65 00 36 00 2d 00 36 00 37 00 35 00 32 00 30 00 32 00 38 00 38 00 63 00 38 00 31 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>25d88f4c-7b49-48e0-a1e6-67520288c81b</Guid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8160	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 33 00 3a 00 35 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T04:23:58Z</CreationTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8258	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8262	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8264	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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F0C.tmp.WERInternalMetadata.xml	8308	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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F6B.tmp.xml	0	4771	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b56739\Report.wer	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b56739\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	172	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_9fb6f77b13131586566dd65310d5dce5865fec4f_82810a17_19b56739\Report.wer	11452	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 39 00 39 00 37 00 35 00 37 00 30 00 30 00 31 00	MetadataHash=1699757001	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d7bac14e-32f2-e498-2810-43a65097fea5}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0D43D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: rundll32.exe PID: 5044, Parent PID: 5568

General

Target ID:	10
Start time:	21:23:59
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\qbot1.dll,m?0BinaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@1@Z
Imagebase:	0x8b0000
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: **7044**, Parent PID: **5044**

General

Target ID:	12
Start time:	21:24:00
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5044 -s 672
Imagebase:	0x180000
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	6C0E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A1A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A1A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1bc56fb5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1bc56fb5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A1A.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A1A.tmp.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A3B.tmp.csv	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B94.tmp.txt	success or wait	1	6C0D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 6e 79 64 fd 05 12 00 00 00 00 00	MDMP nyd	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.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 13 00 00 fd 6e 79 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTnyd0= Pacific Standard TimePacific Daylight T ime	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	8622	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 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 08 fd 67 00 44 76 fd fd 20 08 08 10 40 1c 64 00 fd 66 08 00 23 00 00 00 46 02 01 00 20 1c 64 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++gDv @df#F d+	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	1620	168	fd 1a 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 66 08 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 66 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	ff!	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	11486	20	11 00 00 00 44 4f 3e 00 00 00 00 00 04 00 00 00 fd 2d 00 00	DO>-	success or wait	17	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	11762	4	6b 00 65 00	ke	success or wait	16	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	279814	4096	fd fd fd fd 00 00 fd 02 00 40 fd 02 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 4e 00 00 00 00 00 fd 13 00 00 10 1b 00 00 00 00 00 00 00 00 00 00 00 60 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@N`N	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	9338	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 fd 67 00 fd fd fd fd 20 08 08 10 40 1c 64 00 fd 66 08 00 23 00 00 00 46 02 01 00 20 1c 64 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++g @df#F d+	success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	1888	48	10 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 4e 00 00 00 00 00 fd fd fd 02 00 00 00 00 64 06 00 00 fd 13 04 00 fd 02 00 00 12 2a 00 00	Nd*	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	6596	752	00 00 72 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 5d 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 61 fd 1a 00 00 00 00 00 fd 0f 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 71 42 05 00 00 00 00	rs0Us@!BB? #@AZbF]a@qB	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	283910	9294	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66BC.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 14 01 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 19 00 00 fd 5f 04 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T_0	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 30 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5044</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 31 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1810</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 37 00 34 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123748352</PeakVirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 37 00 34 00 34 00 32 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123744256</VirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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 39 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2395</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 30 00 36 00 30 00 39 00 32 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>8060928</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 30 00 36 00 30 00 39 00 32 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>8060928</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177952</QuotaPeakPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 37 00 37 00 34 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>177744</QuotaPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>25536</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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 35 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>25400</QuotaNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 32 00 34 00 38 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5324800</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 32 00 38 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5328896</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 32 00 34 00 38 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5324800</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5568</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 31 00 36 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5162</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 39 00 32 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>926</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 32 00 33 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3223552</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 31 00 37 00 30 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3117056</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>626688</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>634880</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>626688</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4766	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	18	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5550	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5554	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5556	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5596	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5600	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5602	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	6	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	12	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	5648	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6202	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6206	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6208	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6252	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6254	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6300	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6402	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 79 00 62 00 65 00 68 00 6a 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ybehjb, Inc.</SystemManufacturer>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6516	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 79 00 62 00 65 00 68 00 6a 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ybehjb7,1</SystemProductName>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6620	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6748	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 31 00 30 00 38 00 33 00 35 00 38 00 37 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>1641083587</OSInstallDate>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6830	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6834	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6838	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6944	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	6948	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7022	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7068	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7110	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7212	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7254	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7278	4	0d 00 0a 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7282	2	09 00		success or wait	6	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7286	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7536	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7568	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 34 00 3a 00 30 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T04:24:01Z">	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7676	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 30 00 34 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 32 00 36 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 36 00 35 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="374" PID="5044" UptimeMS="265" TimeSinceCreationMS="265" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7942	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7962	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7966	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	7968	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8012	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8058	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 36 00 30 00 64 00 62 00 65 00 30 00 66 00 2d 00 61 00 34 00 64 00 63 00 2d 00 34 00 37 00 62 00 65 00 2d 00 61 00 61 00 34 00 38 00 2d 00 34 00 36 00 35 00 38 00 33 00 35 00 39 00 32 00 36 00 64 00 64 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>660dbe0f-a4dc-47be-aa48-465835926ddd</Guid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8164	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 34 00 3a 00 30 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T04:24:01Z</CreationTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8268	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER69DA.tmp.WERInternalMetadata.xml	8312	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A1A.tmp.xml	0	4771	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1bc56fb5\Report.wer	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1bc56fb5\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	171	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1bc56fb5\Report.wer	11418	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 30 00 39 00 37 00 31 00 35 00 30 00 30 00 30 00	MetadataHash=1609715000	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0D43D1	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 BE 6B 08 00 02 00 00 00 08 00 00 00 BE 6B 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 88 66 08 00 02 00 00 00 08 00 00 00 88 66 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C0F1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **5772**, Parent PID: **5568**

General

Target ID:	13
Start time:	21:24:02
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\qbot1.dll,m?0BreakpointInfo@ScScript@@QAE@ABV01@@Z
Imagebase:	0x8b0000
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: **7072**, Parent PID: **5772**

General

Target ID:	15
Start time:	21:24:03
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5772 -s 648
Imagebase:	0x180000
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	6C0E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1be17998	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1be17998\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C0D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745B.tmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745B.tmp.xml	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745F.tmp.csv	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75F6.tmp.txt	success or wait	1	6C0D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 6e 79 64 fd 05 12 00 00 00 00 00	MDMP nyd	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.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 16 00 00 fd 6e 79 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTnyd0=Pacific Standard TimePacific Daylight Time	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	8622	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 02 61 fd 02 29 70 fd 07 10 fd 1a fd 02 fd 66 08 00 23 00 00 00 46 02 01 00 fd 1a fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++a)pf#F+	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 66 08 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 66 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	ff!	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	11486	20	10 00 00 00 44 fd fd 02 00 00 00 00 fd 08 00 00 fd 2d 00 00	D-	success or wait	16	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	11746	2236	7c fd 0f 77 34 fd 0e 77 54 02 00 00 fd 07 fd 02 00 00 00 00 fd fd fd fd 40 fd 0d 77 fd 06 fd 02 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd 02 56 0e 77 fd fd fd fd 00 00 00 00 28 08 fd 02 fd 07 fd 02 fd fd fd 02 fd fd fd 02 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 02 fd fd 0d 77 00 00 00 00 fd 06 fd 02 40 fd 0d 77 fd fd fd fd fd fd fd fd 00 00 00 00 fd 07 fd 02 fd fd fd 02 fd fd fd 02 fd fd 0f 77 fd fd fd fd 2f fd 0d 77 fd fd fd 02 fd fd 0d 77 fd fd fd 02 28 08 fd 02 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd 06 fd 02 00 10 fd 02 00 10 fd 02 00 00 00 00 54 02 00 00 fd fd fd fd 54 02 00 00 fd fd fd fd 00 10 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00	|w4wT@ww(w@ww/ww(@w@wTT	success or wait	15	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	284370	4	fd 7b 1a 77	{w	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	9338	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 02 fd fd fd fd 70 fd 07 10 fd 1a fd 02 fd 66 08 00 23 00 00 00 46 02 01 00 fd 1a fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++pf#F+	success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	1888	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 02 00 00 00 00 fd fd 07 03 00 00 00 00 50 04 00 00 fd 36 00 00 fd 02 00 00 12 2a 00 00	@P6*	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	6596	752	00 00 72 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 17 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 25 fd 03 00 00 00 00 00 5d 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 78 0b 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 71 42 05 00 00 00 00	rs0Us@!BB? #@AZbF%]x@qB	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	284374	9294	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER716B.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 04 01 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 19 00 00 74 61 04 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8Tta0	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5772</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1384</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 37 00 34 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123748352</PeakVirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 37 00 34 00 34 00 32 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123744256</VirtualSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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 38 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2387</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 30 00 34 00 38 00 36 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>8048640</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 30 00 34 00 38 00 36 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>8048640</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177952</QuotaPeakPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 37 00 37 00 34 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>177744</QuotaPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>25664</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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 35 00 35 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>25528</QuotaNonPagedPoolUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 35 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5353472</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 35 00 37 00 35 00 36 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>5357568</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 35 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5353472</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5568</Pid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 37 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7784</Uptime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 39 00 35 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>959</PageFaultCount>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 32 00 33 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3223552</PeakWorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 31 00 37 00 30 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3117056</WorkingSetSize>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>626688</PagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>634880</PeakPagefileUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>626688</PrivateUsage>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.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	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4766	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	18	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	9	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5550	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5554	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5556	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5596	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5600	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5602	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	6	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	12	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	5648	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6202	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6206	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6208	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6252	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6254	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6300	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6402	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 79 00 62 00 65 00 68 00 6a 00 62 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ybehjb, Inc.</SystemManufacturer>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6516	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 79 00 62 00 65 00 68 00 6a 00 62 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ybehjb7,1</SystemProductName>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6612	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6616	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6620	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6748	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 31 00 30 00 38 00 33 00 35 00 38 00 37 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>1641083587</OSInstallDate>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6830	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6834	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6838	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6944	2	09 00		success or wait	2	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	6948	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7022	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7068	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7110	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7212	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7254	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7278	4	0d 00 0a 00		success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7282	2	09 00		success or wait	6	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7286	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7536	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7568	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 34 00 3a 00 30 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T04:24:04Z">	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7676	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 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="378" PID="5772" UptimeMS="140" TimeSinceCreationMS="140" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7942	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7962	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7966	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	7968	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8012	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8058	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 64 00 36 00 33 00 63 00 66 00 32 00 30 00 2d 00 62 00 35 00 62 00 63 00 2d 00 34 00 36 00 65 00 30 00 2d 00 39 00 63 00 36 00 32 00 2d 00 31 00 35 00 62 00 63 00 38 00 66 00 66 00 63 00 31 00 63 00 62 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ed63cf20-b5bc-46e0-9c62-15bc8ffc1cb6</Guid>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	2	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8164	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 30 00 34 00 3a 00 32 00 34 00 3a 00 30 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T04:24:04Z</CreationTime>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8268	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER741B.tmp.WERInternalMetadata.xml	8312	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745B.tmp.xml	0	4771	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1be17998\Report.wer	0	2	fd fd		success or wait	1	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1be17998\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	172	6C0D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c6a0b02083f29b4f045509d58da68ab1c531655_82810a17_1be17998\Report.wer	11450	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 32 00 39 00 38 00 33 00 39 00 30 00 34 00 34 00	MetadataHash=829839044	success or wait	1	6C0D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0F36BF	unknown
\REGISTRY\A\{773982ad-9edc-b2b9-b47e-22509337c710}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C0D43D1	unknown

Analysis Process: rundll32.exe PID: **7156**, Parent PID: **5568**

General

Target ID:	16
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",m?0API@ScScript@@IAE@AAVEngine@1@H@Z
Imagebase:	0x8b0000
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: **5444**, Parent PID: **5568**

General	
Target ID:	17
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",m?0BinaryNode@ScScript@@QAE@ABUScanInfo@1@PAVNode@1@1@Z
Imagebase:	0x8b0000
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: **5428**, Parent PID: **5568**

General	
Target ID:	18
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",m?0BreakpointInfo@ScScript@@QAE@ABV01@@Z
Imagebase:	0x8b0000
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: **7020**, Parent PID: **5568**

General	
Target ID:	19
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",next
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000013.00000002.424621480.0000000002C4A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000013.00000002.425037724.0000000004870000.00000004.00000020.00020000.00000000.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: **4604**, Parent PID: **5568**

General	
Target ID:	20
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",munlockRef@Engine@ScScript@@QAEXABVVariant@ScCore@@@Z
Imagebase:	0x8b0000
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: **5668**, Parent PID: **5568**

General	
Target ID:	24
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",mundefinedError@Callback@ScScript@@UAE_NAAVEngine@2@ABVVariant@ScCore@@1AAV45@@Z
Imagebase:	0x8b0000
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: **6504**, Parent PID: **5428**

General	
Target ID:	25
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5428 -s 652
Imagebase:	0x180000
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: **6612**, Parent PID: **7156**

General	
Target ID:	26
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7156 -s 652
Imagebase:	0x180000
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: **6868**, Parent PID: **5444**

General	
Target ID:	27
Start time:	21:24:06
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5444 -s 648
Imagebase:	0x180000
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: **7148**, Parent PID: **7020**

General	
Target ID:	30
Start time:	21:24:11
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x2a0000
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: **2244**, Parent PID: **7148**

General	
Target ID:	32
Start time:	21:27:27
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0x11a0000

File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4332**, Parent PID: **2244**

General

Target ID:	33
Start time:	21:27:27
Start date:	01/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5324**, Parent PID: **7148**

General

Target ID:	34
Start time:	21:27:28
Start date:	01/06/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0x3e0000
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: **5500**, Parent PID: **5324**

General

Target ID:	35
Start time:	21:27:28
Start date:	01/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **5520**, Parent PID: **564**

General	
Target ID:	37
Start time:	21:27:28
Start date:	01/06/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff71f4e0000
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