ID: 755933
Sample Name: New PO-RJ-IN-003 - Knauf Queimados.exe
Cookbook: default.jbs
Time: 10:32:08
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

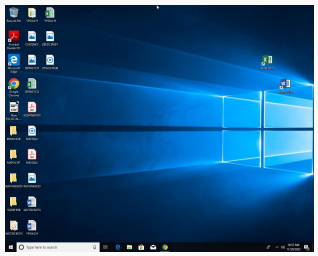
Windows Analysis Report

New PO-RJ-IN-003 - Knauf Queimados.exe

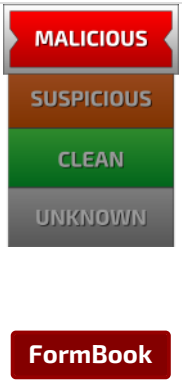
Overview

General Information

Sample Name:	New PO-RJ-IN-003 - Knauf Queimados.exe
Analysis ID:	755933
MD5:	244fc9610f75225..
SHA1:	ef0d6103d27090..
SHA256:	05cdda3567b913..
Tags:	exe
Infos:	



Detection



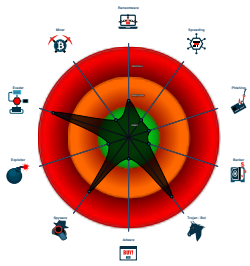
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Performs DNS queries to domains w…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- New PO-RJ-IN-003 - Knauf Queimados.exe (PID: 748 cmdline: C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe MD5: 244FC9610F75225AA3DC09958195BEB1)
  - jaxdij.exe (PID: 1572 cmdline: "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\Local\Temp\uqnwrddys.k MD5: 2DD6C8B13AE7D028B0047435FF0DCB8A)
    - jaxdij.exe (PID: 5360 cmdline: "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\Local\Temp\uqnwrddys.k MD5: 2DD6C8B13AE7D028B0047435FF0DCB8A)
      - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - rubthqnwyfue.exe (PID: 5040 cmdline: "C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe" "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\L MD5: 2DD6C8B13AE7D028B0047435FF0DCB8A)
          - WerFault.exe (PID: 2912 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5040 -s 476 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - rubthqnwyfue.exe (PID: 6040 cmdline: "C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe" "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\L MD5: 2DD6C8B13AE7D028B0047435FF0DCB8A)
          - WerFault.exe (PID: 5420 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 444 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - rundll32.exe (PID: 5412 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.spirituallyzen.com/m9ae/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6601:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f090:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa8af:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17de7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17be5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17691:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17ce7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17e5f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa47a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x168dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1ddf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edfa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a0f9:$sqlite3step: 68 34 1C 7B E1 • 0x1ac71:$sqlite3step: 68 34 1C 7B E1 • 0x1a13b:$sqlite3text: 68 38 2A 90 C5 • 0x1acb6:$sqlite3text: 68 38 2A 90 C5 • 0x1a152:$sqlite3blob: 68 53 D8 7F 8C • 0x1accc:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.417309274.0000000001060000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 25 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.jaxdij.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.jaxdij.exe.400000.1.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x7d38:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x207c7:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbfe6:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1951e:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.2.jaxdij.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1931c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18dc8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1941e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x19596:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xbbb1:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18013:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1f52e:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20531:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.jaxdij.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1b830:$sqlite3step: 68 34 1C 7B E1 • 0x1c3a8:$sqlite3step: 68 34 1C 7B E1 • 0x1b872:$sqlite3text: 68 38 2A 90 C5 • 0x1c3ed:$sqlite3text: 68 38 2A 90 C5 • 0x1b889:$sqlite3blob: 68 53 D8 7F 8C • 0x1c403:$sqlite3blob: 68 53 D8 7F 8C
2.2.jaxdij.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 93.179.127.27	
Timestamp:	192.168.2.593.179.127.2749736802031449 11/29/22-10:35:37.226497
SID:	2031449
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 107.148.15.81	
Timestamp:	192.168.2.5107.148.15.8149749802031453 11/29/22-10:36:16.701501
SID:	2031453
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 107.148.15.81	
Timestamp:	192.168.2.5107.148.15.8149749802031412 11/29/22-10:36:16.701501
SID:	2031412
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 93.179.127.27	
Timestamp:	192.168.2.593.179.127.2749736802031453 11/29/22-10:35:37.226497
SID:	2031453
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 107.148.15.81	
Timestamp:	192.168.2.5107.148.15.8149749802031449 11/29/22-10:36:16.701501
SID:	2031449
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 93.179.127.27	
Timestamp:	192.168.2.593.179.127.2749736802031412 11/29/22-10:35:37.226497
SID:	2031412
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

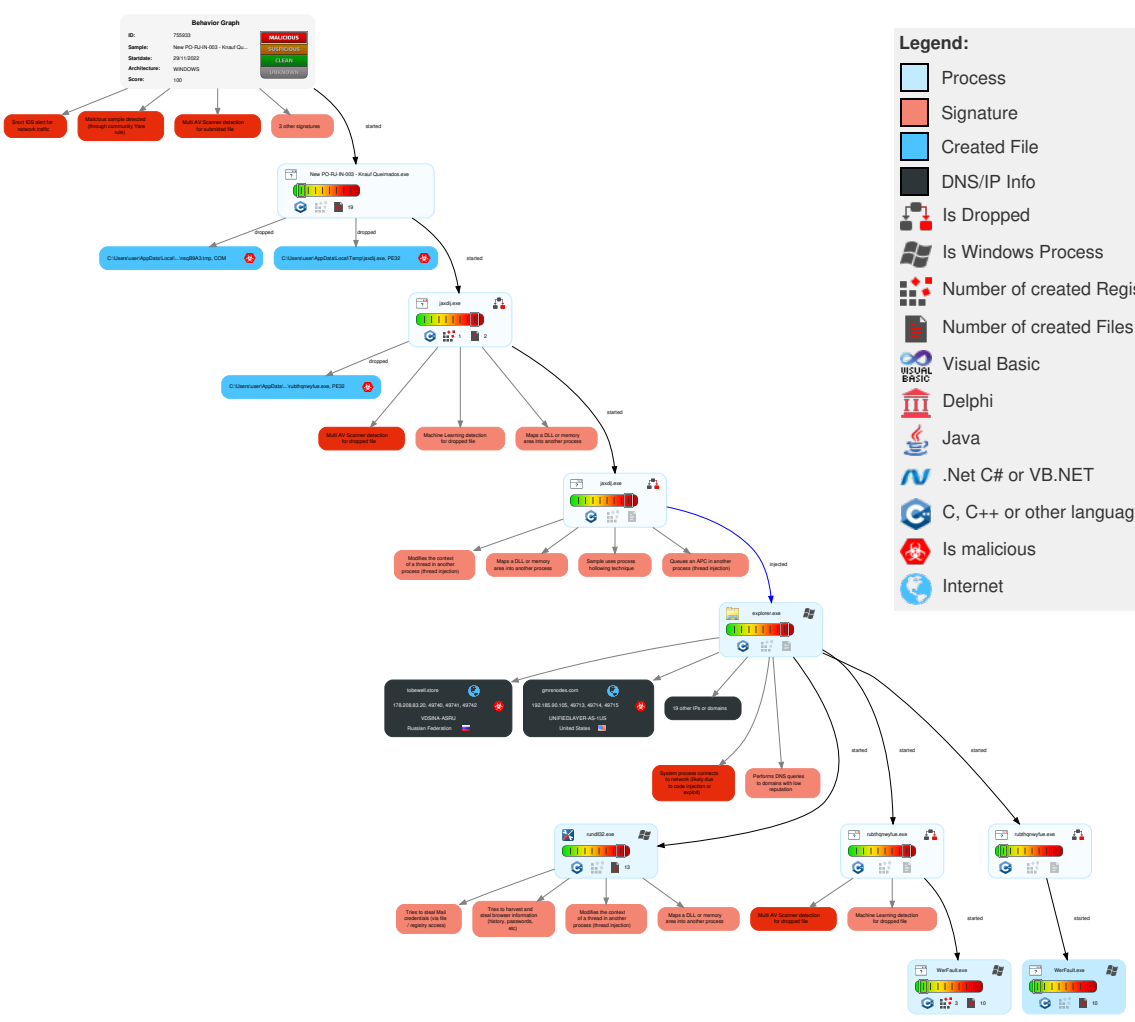
Yara detected FormBook

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	1 Shared Modules	1 Registry Run Keys / Startup Folder	5 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	2 1 Input Capture	2 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Masquerading	Security Account Manager	1 5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Virtualization/Sandbox Evasion	NTDS	1 3 1 Security Software Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	5 1 2 Process Injection	LSA Secrets	2 Virtualization/Sandbox Evasion	SSH	2 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	2 Process 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 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

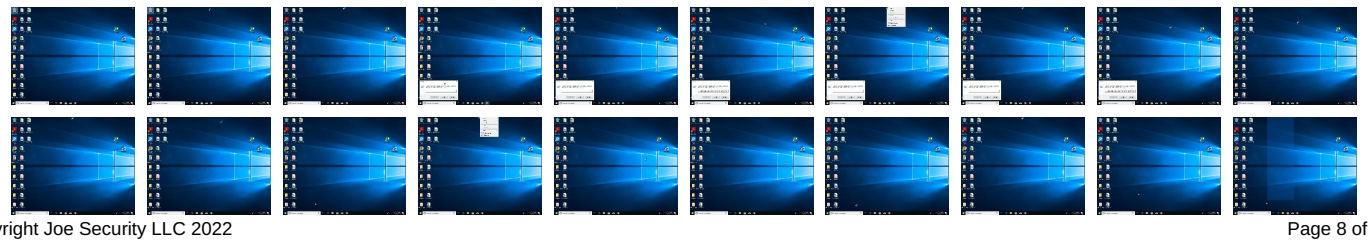
Behavior Graph

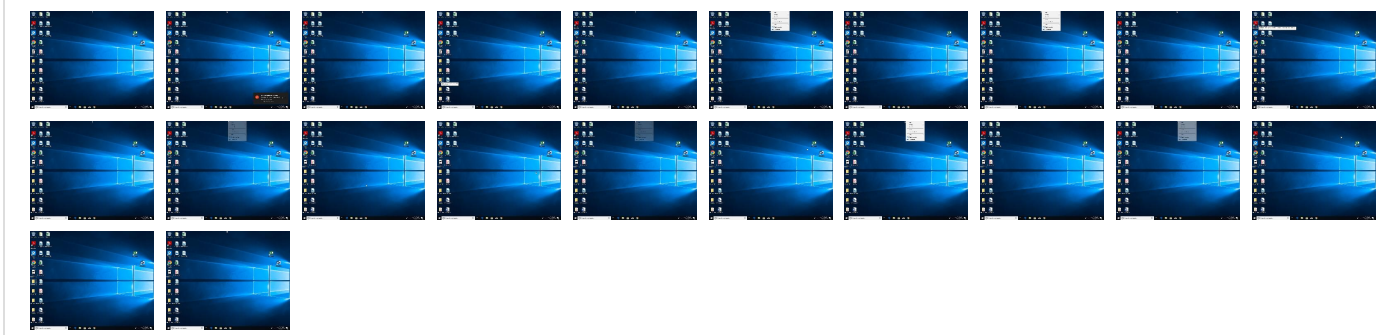


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
New PO-RJ-IN-003 - Knauf Queimados.exe	28%	ReversingLabs	Win32.Trojan.Jaik	
New PO-RJ-IN-003 - Knauf Queimados.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\jaxdij.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\jaxdij.exe	12%	ReversingLabs		
C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe	12%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.New PO-RJ-IN-003 - Knauf Queimados.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
2.2.jaxdij.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.New PO-RJ-IN-003 - Knauf Queimados.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
2.0.jaxdij.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.jaxdij.exe.600000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.spirituallyzen.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.tobewell.store/m9ae/	0%	Avira URL Cloud	safe	
http://www.spirituallyzen.com/m9ae/?F6z4=4ec4fK6CMrtHuja3pViXkl8dlfKAbA0cl+B6ZD+yu2XjTt2h0hV8coMCjgRVKURuW2bGAgNBkAmkGWEjBIBjWi0t+MmK3uNJiA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.amspustaka.com/m9ae/?F6z4=qV5DC7gvSDrvRRGewn1q/l/EwjqoLGbs6Pm0OHOL9iW03iXh+4kaxlrb2hUer6xMCUxzC2FjXkfJjvQV3jFRWlDNN37fVrd03A==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.oonrreward.xyz	0%	Avira URL Cloud	safe	
http://www.frwqc.com/m9ae/?F6z4=pynBU+gmcVJLvmAk24XYTH3CuEH61wNq2RizpB0aNcQM45kGiq+MbQwB99t5gTqC+tvIVg5qQAlCnSYFpOBmFRnmyN3XSGsj5w==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.lee-perez.com/m9ae/?F6z4=nJLDtYwD0af/ePmsJ0ZKjiSVJI8rGVPKc+UQspc6K5yuMKQDKTWfrb6tVbro5/Rq1DJ6W8y/y+8M88qCUODrzxtLw2C30JMyEA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.bookmygennie.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.ybkos.link/m9ae/	0%	Avira URL Cloud	safe	
http://www.tobewell.store/m9ae/?F6z4=IYAlNlE+FJHaxy8xKQwy2r7+8XL3SaTnyfpqtFACBxvA1+IYQm/X+/KTYzdsJPpQzBa/f1IuIPzZtkKHtHHlpgqy4oXa9op1jw==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.amspustaka.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.new-thinking.digital/m9ae/?F6z4=yeGgPnkUyrtnR7ayT+iAJkQi5P+hLqfzRu7/UlGlFriReHTN1+d7DIiWZVVmKJ4cvvB3dwEDWmLuBMYDpMvfxEUSQC8X9wPCmA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.700544.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.lee-perez.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.frwqc.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.bookmygennie.com/m9ae/?F6z4=6mtkb9sgLdU5EKgBox+sPzjX7gz7/N2rxrRH87049lJ0dh9Tn6WPD5ftVfyzJnBGA3PJpfJHiW/BJrwPQwZWSWvRAWejN4CLLw==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://oonrreward.xyz/m9ae/?F6z4=LevhYPqdwsQo7WECD6x58K9v32wKr9jEH/unqFqLlkFUX6m7L7	0%	Avira URL Cloud	safe	
www.spirituallyzen.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.publickit.website/m9ae/?F6z4=XxObD+bozu8R8o86HZoklAwRDcTSUgt1X0zVs8jY2xx2j7amGX2Nanqc4HjuSpD/F/TSiqNoyiNwTcXhTU7ob6qQALfoq6EoqQ==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.tommy57.shop/m9ae/?F6z4=SKemUsRCc/T/1VtJMmoBZUTfzvZVAKOrpHPFHv5bIcLS1NPOlJ3jWavkIE8DT12a+oeWOwZfdDSidPGYCemgiB/muCJBu0rQaA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.dailyheraldresearch.com/m9ae/?F6z4=q+GqSbkO5kqO+W9u2R8uyv/azK/Tyw9Ktq6EIVL87IABA33EfP0KANVapKUQlEGAPHMNZ2Czo2C9EtWkfzzg2b9ydKIDbcUulA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.porggiret.site/m9ae/?F6z4=la9UBuDbTkNYLSjTdKhHvd+t7tYwPiF7FtZOQELnOBzejFZIEJsWuQ55NoeYz7TqoHjnmCP3NdRIHdLBoOXytpXMXLmthCtowg==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.oonrreward.xyz/m9ae/?F6z4=LevhYPqdwsQo7WECD6x58K9v32wKr9jEH/unqFqLIkFUX6m7L7+nio4XOLIDaWup3nHmZdjhK28JVchKAobJnM2R7Dp3tDlOSA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.dailyheraldresearch.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.porggiret.site/m9ae/	0%	Avira URL Cloud	safe	
http://www.ybkos.link/m9ae/?F6z4=19Acn/cRxsS2hMIvbksqz2Fo9/tvE3PmoTWmDY67F7eOm0DJL1plqZyOKvwSm3g2XK4MIkQK6hC8KTphNB2J9vZOQC2YpVwH6g==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.gmrsnodes.com/m9ae/	0%	Avira URL Cloud	safe	
http://www.gmrsnodes.com/m9ae/?F6z4=mwF44ViOu9spAX9yiKWO/GCmf5D0pm7R930/p+8373gvxGpTfL4o/Lm9AHizqU6H72eF1eWgDLpzZ2SfuF6Kyw289k0D2VxhyA==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.700544.com/m9ae/?F6z4=Mu7XrmbNuBpRkVuoTBGU/iHqS/OhVA7Any/uXbqYT12baRfdD/rxJiFT6KJrK4J1cV2pSA20UCfshAzQrgjlnBPfig9iswk20g==&mN6Hg=kRq8Chx0sXs4Nnu0	0%	Avira URL Cloud	safe	
http://www.new-thinking.digital/m9ae/	0%	Avira URL Cloud	safe	
http://www.publickit.website/m9ae/	0%	Avira URL Cloud	safe	
http://www.tommy57.shop/m9ae/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.porggiret.site	198.54.121.81	true	true		unknown
www.dailyheraldresearch.com	172.67.214.243	true	true		unknown
www.ybkos.link	107.148.15.81	true	true		unknown
tobewell.store	178.208.83.20	true	true		unknown
www.tommy57.shop	74.208.236.65	true	true		unknown
www.bookmygennie.com	38.163.214.169	true	true		unknown
www.new-thinking.digital	62.233.121.61	true	true		unknown
www.oonrreward.xyz	188.114.97.3	true	true		unknown
pp.3105.net	93.179.127.27	true	true		unknown
gmrsnodes.com	192.185.90.105	true	true		unknown
www.frwqc.com	38.40.166.195	true	true		unknown
amspustaka.com	23.111.12.177	true	true		unknown
www.spirituallyzen.com	74.208.236.214	true	true		unknown
publickit.website	206.83.40.92	true	true		unknown
www.lee-perez.com	216.40.34.41	true	true		unknown
www.publickit.website	unknown	unknown	true		unknown
www.davidemarone.com	unknown	unknown	true		unknown
www.gmrsnodes.com	unknown	unknown	true		unknown
www.tobewell.store	unknown	unknown	true		unknown
www.700544.com	unknown	unknown	true		unknown
www.amspustaka.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.amspustaka.com/m9ae/?F6z4=qV5DC7gvSDrvRRGewn1q/l/EwjqoLGbs6Pm0OHOL9iW03iXh+4kaxlrb2hUer6xMCUxzC2FjXkfJjvQV3jFRWIDNN37fVrd03A==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
www.spirituallyzen.com/m9ae/	true	• Avira URL Cloud: safe	low
http://www.frwqc.com/m9ae/?F6z4=pynBU+gmcVJLvmAk24XYTH3CuEH61wNq2RizpB0aNcQM45kGiq+MbQwB99t5gTqC+tvIVg5qQAlCnSYFpOBmFRnmyN3XSGsj5w==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.tobewell.store/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.lee-perez.com/m9ae/?F6z4=nJLDtYwD0af/ePmsJ0ZKjiSVJI8rGVPKc+UQspc6K5yuMKQDKTWfrb6tVbro5/Rq1DJ6W8y/y+8M88qCUODrzxtLw2C30JMyEA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.ybkos.link/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.bookmygennie.com/m9ae/	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.spirituallyzen.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.spirituallyzen.com/m9ae/?F6z4=4ec4fK6CMrtHuja3pViXkl8dlfKAbA0cl+B6ZD+yu2XjTt2h0hV8coMCjgRVKURuW2bGAgNBkAmkGWEjBIBjWi0t+MmK3uNJiA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.amspustaka.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.tobewell.store/m9ae/?F6z4=IYAlNlE+FJHaxy8xKQwy2r7+8XL3SaTnyfpqtFACBxvA1+IYQm/X+/KTYzdsJPpQzBa/f1IuIPzZtkKHtHHlpgqy4oXa9op1jw==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.lee-perez.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.700544.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.new-thinking.digital/m9ae/?F6z4=yeGgPnkUyrtnR7ayT+iAJkQi5P+hLqfzRu7/UlGlFriReHTN1+d7DIiWZVVmKJ4cvvB3dwEDWmLuBMYDpMvfxEUSQC8X9wPCmA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.bookmygennie.com/m9ae/?F6z4=6mtkb9sgLdU5EKgBox+sPzjX7gz7/N2rxrRH87049lJ0dh9Tn6WPD5ftVfyzJnBGA3PJpfJHiW/BJrwPQwZWSWvRAWejN4CLLw==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.frwqc.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.publickit.website/m9ae/?F6z4=XxObD+bozu8R8o86HZokIAwRDcTSUgt1X0zVs8jY2xx2j7amGX2Nanqc4HjuSpD/F/TSiqNoyiNwTcXhTU7ob6qQALfoq6EoqQ==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.tommy57.shop/m9ae/?F6z4=SKemUsRCc/T/1VtJMmoBZUTfzvZVAKOrpHPFHv5bIcLS1NPOlJ3jWavkIE8DT12a+oeWOwZfdDSidPGYCemgiB/muCJBu0rQaA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.dailyheraldresearch.com/m9ae/?F6z4=q+GqSbkO5kqO+W9u2R8uyv/azK/Tyw9Ktq6EIVL87IABA33EfP0KANVapKUQlEGAPHMNZ2Czo2C9EtWkfzzg2b9ydKIDbcUulA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.dailyheraldresearch.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.porggiret.site/m9ae/?F6z4=la9UBuDbTkNYLSjTdKhHvd+t7tYwPiF7FtZOQELnOBzejFZIEJsWuQ55NoeYz7TqoHjnmCP3NdRIHdLBoOXytpXMXLmthCtowg==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.oonrreward.xyz/m9ae/?F6z4=LevhYPqdwsQo7WECD6x58K9v32wKr9jEH/unqFqLlkFUX6m7L7+nio4XOLlDaWup3nHmZdjhK28JVchKAobJnM2R7Dp3tDlOSA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.ybkos.link/m9ae/?F6z4=19Acn/cRxsS2hMIvbksqz2Fo9/tvE3PmoTWmDY67F7eOm0DJL1plqZyOKvwSm3g2XK4MIkQK6hC8KTphNB2J9vZOQC2YpVwH6g==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.porggiret.site/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.gmrsnodes.com/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.gmrsnodes.com/m9ae/?F6z4=mwF44ViOu9spAX9yiKWO/GCmf5D0pm7R930/p+8373gvxGpTfL4o/Lm9AHizqU6H72eF1eWgDLpzZ2SfuF6Kyw289k0D2VxhyA==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.700544.com/m9ae/?F6z4=Mu7XrmbNuBpRkVuoTBGU/iHqS/OhVA7Any/uXbqYT12baRfdD/rxJiFT6KJrK4J1cV2pSA20UCfshAzQrgjlnBPfig9iswk20g==&mN6Hg=kRq8Chx0sXs4Nnu0	true	• Avira URL Cloud: safe	unknown
http://www.new-thinking.digital/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.publickit.website/m9ae/	true	• Avira URL Cloud: safe	unknown
http://www.tommy57.shop/m9ae/	true	• Avira URL Cloud: safe	unknown

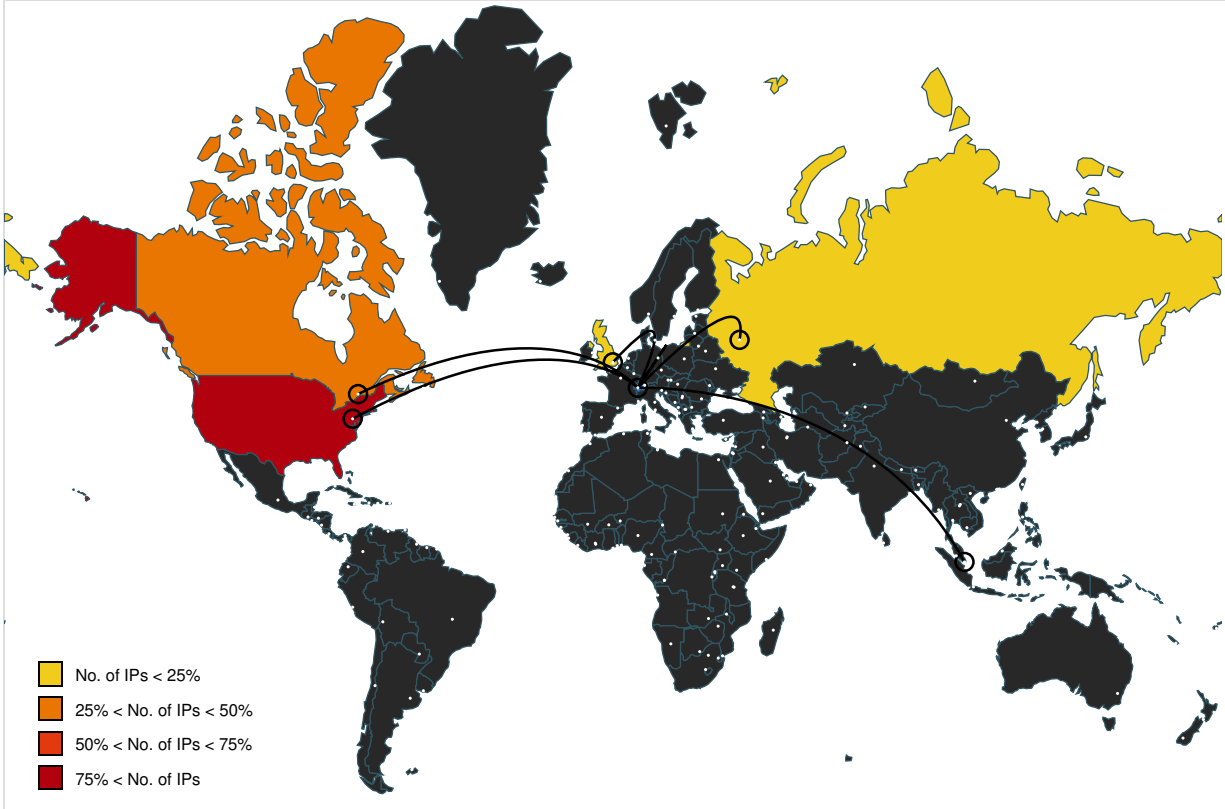
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	rundll32.exe, 0000000B.00000003.48504444 1.0000000007231000.00000004.00000800.000 20000.00000000.sdmp, 456b6ELMQ.11.dr	false		high
http://https://duckduckgo.com/ac/?q=	456b6ELMQ.11.dr	false		high
http://https://www.instagram.com/hover_domains	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://supportservices.easyspace.com/	rundll32.exe, 0000000B.00000002.82418760 5.0000000005D7A000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://controlpanel.easyspace.com/	rundll32.exe, 0000000B.00000002.82418760 5.0000000005D7A000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	rundll32.exe, 0000000B.00000003.48504444 1.0000000007231000.00000004.00000800.000 20000.00000000.sdmp, 456b6ELMQ.11.dr	false		high
http://https://www.easyspace.com/assets/images/structure/easyspace-logo-main.svg	rundll32.exe, 0000000B.00000002.82418760 5.0000000005D7A000.00000004.10000000.000 40000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hover.com/email?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.hover.com/about?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.oonrreward.xyz	rundll32.exe, 0000000B.00000002.82350867 3.0000000004DC6000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.hover.com/domains/results	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://oonrreward.xyz/m9ae/?F6z4=LevhYPqdwsQo7WECD6x58K9v32wKr9jEH/unqFqLlkFUX6m7L7	rundll32.exe, 0000000B.00000002.82350867 3.0000000004DC6000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.hover.com/tools?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://help.hover.com/home?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://code.jquery.com/jquery-3.3.1.min.js	rundll32.exe, 0000000B.00000002.82353805 5.0000000004F58000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://www.hover.com/domain_pricing?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.hover.com/privacy?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.31354643 6.0000000000921000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.391112959.000000000091F000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.361885332.000000 000091F000.00000004.00000020.00020000.00 000000.sdmp	false		high
http://https://twitter.com/hover	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	rundll32.exe, 0000000B.00000003.48504444 1.0000000007231000.00000004.00000800.000 20000.00000000.sdmp, 456b6ELMQ.11.dr	false		high
http://https://www.hover.com/transfer_in?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.easyspace.com/	rundll32.exe, 0000000B.00000002.82418760 5.0000000005D7A000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://www.hover.com/renew?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css	rundll32.exe, 0000000B.00000002.82418760 5.0000000005D7A000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	456b6ELMQ.11.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mchost.ru/	rundll32.exe, 0000000B.00000002.82408555 5.0000000005BE8000.00000004.10000000.000 40000.00000000.sdmp	false		high
http:// https://search.yahoo.com/favicon.icohttps://search.yah oo.com/search	rundll32.exe, 0000000B.00000003.48504444 1.0000000007231000.00000004.00000800.000 20000.00000000.sdmp, 456b6ELMQ.11.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	New PO-RJ-IN-003 - Knauf Queimados.exe	false		high
http://https://search.yahoo.com/sugg/chrome? output=fxjson&appid=crmas_sfp&command=	rundll32.exe, 0000000B.00000003.48504444 1.0000000007231000.00000004.00000800.000 20000.00000000.sdmp, 456b6ELMQ.11.dr	false		high
http://gmpg.org/xfn/11	rundll32.exe, 0000000B.00000002.82353805 5.0000000004F58000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	456b6ELMQ.11.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	rundll32.exe, 0000000B.00000003.48504444 1.0000000007231000.00000004.00000800.000 20000.00000000.sdmp, 456b6ELMQ.11.dr	false		high
http://nsis.sf.net/NSIS_Error	New PO-RJ-IN-003 - Knauf Queimados.exe	false		high
http://https://www.hover.com/tos?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttp s://www.ecosia.org/search?q=	456b6ELMQ.11.dr	false		high
http://https://www.hover.com/?source=parked	rundll32.exe, 0000000B.00000002.82374646 4.000000000540E000.00000004.10000000.000 40000.00000000.sdmp, rundll32.exe, 00000 00B.00000002.824795992.0000000006FA0000. 00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.83.40.92	publickit.website	Canada		207083	HOSTSLIM-GLOBAL-NETWORKNL	true
107.148.15.81	www.ybkos.link	United States		54600	PEGTECHINCUS	true
74.208.236.65	www.tommy57.shop	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
93.179.127.27	pp.3105.net	Canada		25820	IT7NETCA	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.111.12.177	amspustaka.com	Singapore		33438	HIGHWINDS2US	true
74.208.236.214	www.spirituallyzen.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
38.40.166.195	www.frwqc.com	United States		174	COGENT-174US	true
192.185.90.105	gmrsnodes.com	United States		46606	UNIFIEDLAYER-AS-1US	true
62.233.121.61	www.new-thinking.digital	United Kingdom		20860	IOMART-ASGB	true
188.114.97.3	www.oonrreward.xyz	European Union		13335	CLOUDFLARENETUS	true
178.208.83.20	tobewell.store	Russian Federation		48282	VDSINA-ASRU	true
38.163.214.169	www.bookmygennie.com	United States		174	COGENT-174US	true
172.67.214.243	www.dailyheraldresearch.com	United States		13335	CLOUDFLARENETUS	true
216.40.34.41	www.lee-perez.com	Canada		15348	TUCOWSCA	true
198.54.121.81	www.porggiret.site	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755933
Start date and time:	2022-11-29 10:32:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New PO-RJ-IN-003 - Knauf Queimados.exe
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/14@19/15
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 72.4% (good quality ratio 62.7%) • Quality average: 70.8% • Quality standard deviation: 35.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 20.189.173.21
- Excluded domains from analysis (whitelisted): client.wns.windows.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- 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 getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:33:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run aekkvxebyca C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\L
10:33:15	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run aekkvxebyca C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\L
10:33:24	API Interceptor	2x Sleep call for process: WerFault.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_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_0b3f82dd\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):	0.8402962355282704
Encrypted:	false
SSDEEP:	96:G2F7LbmubhHJ76f5pXIQcQvc6QcEDMcw3DD+HbHg/EFAeugtYsaV9w72n2/AopgQ:BBOLHBUZMXgjzxq/u7sdS274lt0
MD5:	6483B1F032E7C7A2064F3902C60460C5
SHA1:	308780D73090910FB14EFD18F7EC0F579D5F6AC8
SHA-256:	309CD45651DC1A312A62DB06F88BC948F67A9BEF2B132F7EB2C3F24D9312A71C
SHA-512:	25FFAE39FE38336C06B08169C325B91D7CF4F1706348BAF060905D06EC6D1AB538D79284835EFD2ECADD0D54747F704DE17F7B3A5875E4D86871B6A7578FF73
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.4.2.2.0.4.0.1.2.7.8.8.3.4.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.4.2.2.0.4.0.2.7.7.8.8.1.0.9.....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.=.0.1.b.3.4.2.0.2.-.4.4.b.5.-.4.d.b.7.-.9.f.b.7.-.8.c.0.a.0.c.0.e.a.2.9.6.....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.=.f.0.2.4.8.2.6.1.-.7.9.5.0.-.4.4.a.c.-.9.5.6.a.-.2.d.b.b.6.8.1.b.a.e.6.3.....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.b.t.h.q.n.w.y.f.u.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.b.0.-.0.0.0.1.-.0.0.1.9.-.2.8.8.1.-.7.1.0.b.2.1.0.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.6.1.2.6.1.e.6.4.c.7.d.b.d.3.f.3.f.b.2.4.a.d.3.1.c.c.6.2.2.5.d.0.0.0.0.f.f.f.f.!.0.0.0.0.d.5.0.b.c.8.8.3.4.7.5.8.e.1.5.8.3.a.e.e.7.2.9.b.6.c.1.4.8.e.4.8.4.9.9.6.7.0.9.7.!.r.u.b.t.h.q.n.w.y.f.u.e...e.x.e.....T.a.r.g.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_15731f22\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):	0.8330437811334652
Encrypted:	false
SSDEEP:	96:NF4F7bmMbhHJ76f5pXIQcQvc6QcEDMcw3DD+HbHgE+5JHQ0DFF8WpsvVv05omZtv:NOUJHBUZMXgjkJq/u7sdS274lt0
MD5:	EA4872801B7758ABB5B9724582927345
SHA1:	C8A3B4E7DA468965CE8EFDE4B9AFA0897DDA8C19
SHA-256:	623023C565AA132FE1174E1E1774BCE708E94940B1FBD45464DB6280EEC15CB0
SHA-512:	C81CF8AC5D1A18C906D967B466550CF69A3CFD3D0B7FD6887AA25C87235C6BBD64665C3B4D006FEBC73A9B93230F3258D96C39EB9A0B4A38D78FEADE6FA45DB0
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.4.2.2.0.4.0.6.6.9.1.4.0.9.9.....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.=.1.3.3.1.4.2.2.0.4.0.8.2.3.8.2.7.6.2.....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.=.0.4.7.8.1.7.5.3.-.9.9.9.b.-.4.2.1.3.-.a.d.3.5.-.8.7.5.2.a.e.d.a.c.2.4.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.=.e.a.8.6.e.b.7.e.-.7.d.8.c.-.4.3.c.f.-.b.5.0.a.-.a.f.4.a.3.0.b.1.e.9.c.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.b.t.h.q.n.w.y.f.u.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.9.8.-.0.0.0.1.-.0.0.1.9.-.3.9.0.c.-.9.a.1.0.2.1.0.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.6.1.2.6.1.e.6.4.c.7.d.b.d.3.f.3.f.b.2.4.a.d.3.1.c.c.6.2.2.5.d.0.0.0.0.f.f.f.f.!.0.0.0.0.d.5.0.b.c.8.8.3.4.7.5.8.e.1.5.8.3.a.e.e.7.2.9.b.6.c.1.4.8.e.4.8.4.9.9.6.7.0.9.7.!.r.u.b.t.h.q.n.w.y.f.u.e...e.x.e.....T.a.r.g.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Nov 29 18:33:27 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	38124
Entropy (8bit):	2.1135243060973754
Encrypted:	false
SSDEEP:	192:lJLLUnttqrOl5vBZrWYMkumjuFCl/wXEX7:bciyILRXMkumj/loE
MD5:	4BB1A8465A8E8CC0512777E6E2FCACF2
SHA1:	D0AB572DED8BD72E988B0EF7ABCDD5A061DCE1BB
SHA-256:	73D48BEA30E4D193508EF8C7DDFED7527CF3CED302B7EF0A5B232932B321B850
SHA-512:	F279B695567203BE277AE105A636163EC2F41B900E94CD934FA26ABE19EA912D755C3F144DF4F4FC044639F2AC5CA10446A1793BF1EDFDC29A9577836C96F20
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....wP.c.....%.....T.....8.....T.....U.....B.....8.....GenuineIntelW.....T.....tP.c..... .....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\WER1753.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):	8316
Entropy (8bit):	3.6971504734754745
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi1h6+kGE76YBScSUvgmfYSSCprm89bPRsf6lm:RrlsNiz6+kGE76YBZSUvgmfYSlPKfx
MD5:	0C2AA2BEACEC714648312E4758CC6398
SHA1:	D0B12EB6E0D73080570C74BD6A89A128619D448E
SHA-256:	8F1FBF663B7649EEC73BBA5BE84352F37F68EEB7D56824A84070722740305BDE
SHA-512:	3B0E18674E59C84C89F875D8CE6E66F0A943EC0498DEA85B41FF28AEE60C620CBBF4E337333BC6E10F30F248878F4D8DE160C404F5228FBAD6D93F6CA0319A09
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.0.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1810.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4577
Entropy (8bit):	4.456911385463713
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqrJgtWl9syWgc8sqYjG8fm8M4JhhYM7aFAO+q8AxF/ucnLGq3131d:ulTfqFvTgrsqYXJhh9fOxxAcnLz3131d
MD5:	787E667FEA93058BAABB354313A383EA
SHA1:	EBE6B5FEF5282B1A9C48E51A4009C84BB7F60EBA
SHA-256:	DA14B3F4C5FE0CAB3583006C73483CEB04A9ADE3558750569B8BBD30C0EB2DCA
SHA-512:	033E73DCB8DDB5BA108A6D6693EA53E19F8B07D44BD7EEB5D504C0518B34C7F80AD5EB76A73E3D4F00F3CF23016F426F9BF0256B00E2668EEE546203968219C 9
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1801664" />.. <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\WER206.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):	8304
Entropy (8bit):	3.699302336059976
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2c6enNL0xq6YBSLSUKgmfYSSCprJ89b5ksfY+zm:RrlsNit6ENL0xq6YBuSUKgmfYSc5XfYL
MD5:	34D0C29EDEB9291888F5D1A50A014FEF
SHA1:	B7821B75BDF77EB93EA9A6F46BD51D9D9A3415FE
SHA-256:	A4A9F780CABA96FAF2230242D42E1DBD129EF0EA355A35805CC8F18D9B61900E
SHA-512:	87A94E5F65571D28D1B4189AE52E5E82AC7C6C14967B2DDD098B5010745B57CAC979A3AA1AC3B041B0B87CF2F871F38568D6229D93378E43E7D042763CFC32E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.0.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A3.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4577
Entropy (8bit):	4.457629089404613
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqrJgtWl9syWgc8sqYj18fm8M4JhhYM7aFz2+q8AxF/5LGq3139d:ulTfqFvTgrsqYGJhh9A2xxLLz3139d
MD5:	62377028B54AEE8D136411AB5EABFB35
SHA1:	4CA2C3D9E7E1DE5292BFCB850BF09CD0E785DD0C
SHA-256:	5E5B155E3AE0838AD92071C53510DF5BC0F8169EE6224BC2BB757C7D67858150
SHA-512:	DB093BCC43A7707163F531332DE4AEFAE40A992EE1D4041499318DAD730A8A9FA6422AFDE03F2E2CEC764EC6DD5AB3CD804BFC22A0EDEA4F8C1588793A132 186
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1801664" />.. <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\WERFF75.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Nov 29 18:33:21 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40132
Entropy (8bit):	2.0040008468253996
Encrypted:	false
SSDEEP:	192:zbmX3FvVpOc5NcFNwpPsf1TFC9GrEBopK:+licrcFNyPs9TjK
MD5:	106AFACC119E90AC953EEABE57CEA3B4
SHA1:	A6ABBED87500BFE854024C5341771C65692FD7FD
SHA-256:	38475C67FD546492D1F7D6D3350CD6F329A101B380E26B2FEC0ED5D67253751B
SHA-512:	3071D8D628D6CC3E0AD05BFD4F1CE80A235CF444CD4966B52E3173C31DC0220150A947B74FF027C879735F865C8D7ABE202F91194415ADBB2E504F94FDFE94F A
Malicious:	false
Preview:	MDMP..... .....qP.c.....p&.....T.....8.....T..... ....U.....B.....GenuineIn telW.....T.....kP.c..... .....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:\Users\user\AppData\Local\Temp\456b6ELMQ

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.287139506398081
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3 1
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\eojsm.wx

Process:	C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.998554091662563**
Encrypted:	**true**
SSDEEP:	3072:SWMXxgX4d9iRFy0ALl5gXs0CQ1/zhvFpaIFNTTzVhqOD/AKuhoTQnnEftVzJJ1IA:RMGFKLl5As+zhGXlYAuhXnnEjFic
MD5:	8C5E7C152ED8F18A0B9DE322E94A3CE2
SHA1:	35C05FA705DC9E6C1998F53F248E0332BC4FB0E2
SHA-256:	B0950EC5415DCFC9BF3394770C2071FAD57B1A02E28416E5E41C3B13266A720A
SHA-512:	0A42DAC7F56CF6B765A52F230C3F1539940F0D507D8CE1C928D89D12BF675F3C41B7B9D9FA10A693ECE96A281DBD8E83D481D310F5CA57812FB979DF34A69C 2
Malicious:	false
Preview:	..{;*_....].3.P NZ.I.3...y.GJs'.j.S+.<ERq.?...$...C.... v....W.....=D@.g..K..s...J.....D..Y.].vM...HG..../.....2F.%R..~...c.4.!.Y+..oj.....3q6.40...&...P..>Zb=d.A+.a... .w"b}... VAzL.uDJ..Q.3.i....x..7|.a..N*..Km..A..7%.(.[....;Ph.....O.....R.GO.@.V_...:){}d_.....lk.....O..:'..SD.<ER..?Y..$...x.... v.(...T...2K.e9..u..oo.....2J.....`.u\.>.t+s..r..2....4fD..3R..~..... <....N...uM#..L=.{. ....!.....7...V.}#.. .w"b}....C.L.uOG<.r..3...x..7|...c..8.K$.....7%.(.....Ph....O.....G..@.V_...){}d_.....lkc....O..Js'.j.S+.<ERq.?...$...C.... v.(...T...2K.e9..u..oo.... .2J.....`.u\.>.t+s..r..2....4fD..3R..~.....<....N...uM#..L=.{. ....!.....7...V.}#.. .w"b}...VAzL.uaz.r..3.sK...x..7|...c..8.Km..A..7%.(.....Ph....O.....G..@.V_...){}d_.....lkc....O..Js'.j.S+. <ERq.?...$...C.... v.(...T...2K.e9..u..oo.....2J.....`.u\.>.t+s..r..2....4fD..3R..~.....<....N...uM#..L=.{. ....!.....7...V.}#.. .w"b}...VAzL.uaz.r..3.sK...x..7|...c..8.Km..A..7%.(.

C:\Users\user\AppData\Local\Temp\jaxdij.exe

Process:	C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	147968

Entropy (8bit):	6.182679953719657
Encrypted:	false
SSDEEP:	3072:jOPPLcLP9kkaQ+nBwmbePxRC/fkBYcgcg7JkWmjwaY4Y4O1JXy:jiLcLP9c/8BZgFLm8FLC
MD5:	2DD6C8B13AE7D028B0047435FF0DCB8A
SHA1:	D50BC8834758E1583AEE729B6C148E4849967097
SHA-256:	01CB657E996E468706F5C733853419678B8294E7F12669C98DB23C1F0D0EFC7A
SHA-512:	B6438EAFA008519CD2113FD113192F2F9F5F05AD5EFBEB08542C800B7E3BD0E7D3DDE83EBBA8A2374E2DF62FED6CC1248B41CE8CEA41BEE256DA8A0B25FCAF2C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 12%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....c.....!.....@.....@.....@.....`.....\|.....text..... ..`.rdata..$t.....v.....@..@.data....%...@.....@....00cfg.....p.....&.....@..@.voltbl."....(.....rsrc.....*.....@..@.reloc.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\nsqB9A3.tmp

Process:	C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	353762
Entropy (8bit):	7.44582442154262
Encrypted:	false
SSDEEP:	6144:dTMGFKLl5As+zhGXlYAuhXnnEjFiREKiLcLP9c/8BZgFLm8FLC:dMGgL3As+gSAu8FuEKiLcLPKcWC8c
MD5:	6B34F2B63558A2CC41B3CB5AF526EC23
SHA1:	8877B4A75BD7DD4DE02CC16643E2AA2E0C193D78
SHA-256:	9C8ACF6A541EE2C83930C4CF4D0E682AE8FFDAF4FCC9FDC244ACCF37416F75A8
SHA-512:	B42DEE735681A9A552F5840AF130D483A5BA2E7FBC6233D5747DA45706166F463E6A49979A0D99B8E4B3B7D6E4C729F43735CF8C1A108FC0C5C8D73B0DFC6ED
Malicious:	**true**
Preview:	.!.....,.....h...T..... .....!.....J.....r...j.....r.....

C:\Users\user\AppData\Local\Temp\uqnwrddys.k

Process:	C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe
File Type:	data
Category:	dropped
Size (bytes):	7706
Entropy (8bit):	6.249721264956451
Encrypted:	false
SSDEEP:	192:xgj/PNnh4pnxYvcIrL+S3yfMae9h4OLzHUphGmKN33w2:xgjnl1xYvReS3yctzHlpKN1
MD5:	A342BD922F1907E57D17E98F522B64EF
SHA1:	934596A7680633634741A445C5D9E0BDCF9C3D8F
SHA-256:	1C1AD949B639CDD656A62B398660A1CCEE4A7FC40E1912BF1A5BBAB78E51B176
SHA-512:	6527A40317BC37D0E7274A3880A652E9BD0EE4E874DEF4478493D93BEE7DB4564CAFEC1574E8605945758963945AADC1D3219410CB877E0C331CECA6671A06AE
Malicious:	false
Preview:	.....(s.....|I...(s.....7....z...gT.....7..T.....56/J.....7.R.....BC.S...L.E.C.V..Jg.7.56/J.....(s.....|,.....gT....."..D.<.T.'.KI.TKI....'....gT....g:.~....g....D.....7.56/J.....M.....=.....|.E.....'.gT.{..Z.M....'..z....7....T561KJ...'..].$....M.....(s.....\|,.s>..7.....<../..9.7....9.7".....9gT.1.'..M.'..]x.]..J"{....U.T.]..J2..B..U"{.....6.]D..F.I..D..=7...../..M...../....<.'.._.T...T.561KJ.....7.R.....BC.S.....L.E.C.]..Jg.7.56/J....."..",..'@..".."...'F."3..':."$..'8."+..'>."...'<...'."(...'..T./....D.....'.....,.i>.....,..P...@.D....,.....,..O...'....,..X...'..~....,.....'.....,.....'.....,..>...'.....7..'..>.....,....".",....7....."....g..5",...ES.....'.gT.....gT.....,...."..",....7.....'...7....gT.....I...T561KJ....."..".."...g...."...g....."..".."...g....."...g2...."'..g0...."

C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe

Process:	C:\Users\user\AppData\Local\Temp\jaxdij.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	147968
Entropy (8bit):	6.182679953719657
Encrypted:	false

SSDEEP:	3072:jOPPLcLP9kkaQ+nBwmbePxRC/fkBYcgcg7JkWmjwaY4Y4O1JXy:jiLcLP9c/8BZgFLm8FLC
MD5:	2DD6C8B13AE7D028B0047435FF0DCB8A
SHA1:	D50BC8834758E1583AEE729B6C148E4849967097
SHA-256:	01CB657E996E468706F5C733853419678B8294E7F12669C98DB23C1F0D0EFC7A
SHA-512:	B6438EAFA008519CD2113FD113192F2F9F5F05AD5EFBEB08542C800B7E3BD0E7D3DDE83EBBA8A2374E2DF62FED6CC1248B41CE8CEA41BEE256DA8A0B25FCAF2C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 12%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....c.....!.....@.....@.....@.....`.....\|.....text..... ..`.rdata..$t.....v.....@..@.data....%...@.....@....00cfg.....p.....&.....@..@.voltbl."....(.....rsrc.....*.....@..@.reloc.....,.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.365597808064567
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	New PO-RJ-IN-003 - Knauf Queimados.exe
File size:	405670
MD5:	244fc9610f75225aa3dc09958195beb1
SHA1:	ef0d6103d27090fc9d25e3ef3de2e1b6d9670d9c
SHA256:	05cdda3567b913d99627f8e41336404d5830816df65e1001d6b2ad05bd9ed18d
SHA512:	5e37d34becf476a92c2b14917819c9f9366d99313e971554b4a94d4fe09e05a761355033b5bb59faf3d0a1e34621c31891ff4e5656a379aa581792a7ecc82f16
SSDEEP:	6144:hBn7A5jMUCoQUg+p1vrgTr+H9l/LKUsBdVyXMLCMT5u9AG7Nmf:vrZ+1v0TSdcLKj0MLtlu9VNG
TLSH:	9284CFA3F245989ED44202B3846EED342612ADAAA435DD1673E6BC3F79F31831463F17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...ly.V.....^.....

File Icon

Icon Hash:	b4b0c6c6c4dedca3

Static PE Info

General

Entrypoint:	0x40324f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796C [Sun Dec 27 05:38:52 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ab6770b0a8635b9d92a5838920cfe770

Entrypoint Preview
Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+1Ch], ebx
mov dword ptr [esp+14h], 00409130h
xor esi, esi
mov byte ptr [esp+18h], 00000020h
call dword ptr [004070B8h]
call dword ptr [004070B4h]
cmp ax, 00000006h
je 00007F6FC0C9C953h
push ebx
call 00007F6FC0C9F741h
cmp eax, ebx
je 00007F6FC0C9C949h
push 00000C00h
call eax
push 004091E0h
call 00007F6FC0C9F6C2h
push 004091D8h
call 00007F6FC0C9F6B8h
push 004091CCh
call 00007F6FC0C9F6AEh
push 0000000Dh
call 00007F6FC0C9F711h
push 0000000Bh
call 00007F6FC0C9F70Ah
mov dword ptr [00423F84h], eax
call dword ptr [00407034h]
push ebx
call dword ptr [00407270h]
mov dword ptr [00424038h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007F6FC0C9F341h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007F6FC0C9F32Fh
push ebx
call dword ptr [00407144h]

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73cc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x1d8a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.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	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x1d8a8	0x1da00	False	0.27741791930379744	data	4.920016096491695	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d280	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536, resolution 4724 x 4724 px/m	English	United States
RT_ICON	0x3daa8	0x4b6e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x42618	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384, resolution 4724 x 4724 px/m	English	United States
RT_ICON	0x46840	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 4724 x 4724 px/m	English	United States
RT_ICON	0x48de8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 4724 x 4724 px/m	English	United States
RT_ICON	0x49e90	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 4724 x 4724 px/m	English	United States
RT_DIALOG	0x4a2f8	0x100	data	English	United States
RT_DIALOG	0x4a3f8	0x11c	data	English	United States
RT_DIALOG	0x4a518	0x60	data	English	United States
RT_GROUP_ICON	0x4a578	0x5a	data	English	United States
RT_MANIFEST	0x4a5d8	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, GetTempPathA, GetCommandLineA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, LoadLibraryA, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, WaitForSingleObject, ExitProcess, GetWindowsDirectoryA, GetProcAddress, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, WriteFile, MulDiv, LoadLibraryExA, GetModuleHandleA, MultiByteToWideChar, FreeLibrary
USER32.dll	GetWindowRect, EnableMenuItem, GetSystemMenu, ScreenToClient, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetForegroundWindow, PostQuitMessage, RegisterClassA, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, OpenClipboard, TrackPopupMenu, SendMessageTimeoutA, GetDC, LoadImageA, GetDlgItem, FindWindowExA, IsWindow, SetClipboardData, SetWindowLongA, EmptyClipboard, SetTimer, CreateDialogParamA, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteValueA, SetFileSecurityA, RegOpenKeyExA, RegDeleteKeyA, RegEnumValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

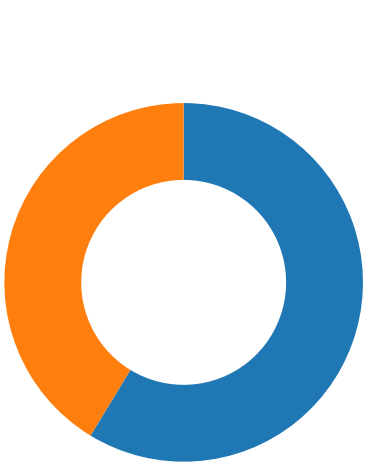
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.593.179.127.27 49736802031449 11/29/22-10:35:37.226497	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	93.179.127.27
192.168.2.5107.148.15.81 49749802031453 11/29/22-10:36:16.701501	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.5	107.148.15.81
192.168.2.5107.148.15.81 49749802031412 11/29/22-10:36:16.701501	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.5	107.148.15.81
192.168.2.593.179.127.27 49736802031453 11/29/22-10:35:37.226497	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	93.179.127.27
192.168.2.5107.148.15.81 49749802031449 11/29/22-10:36:16.701501	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.5	107.148.15.81
192.168.2.593.179.127.27 49736802031412 11/29/22-10:35:37.226497	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	93.179.127.27

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:34:27.048527956 CET	49711	80	192.168.2.5	188.114.97.3
Nov 29, 2022 10:34:27.065722942 CET	80	49711	188.114.97.3	192.168.2.5
Nov 29, 2022 10:34:27.065875053 CET	49711	80	192.168.2.5	188.114.97.3
Nov 29, 2022 10:34:27.138349056 CET	49711	80	192.168.2.5	188.114.97.3
Nov 29, 2022 10:34:27.155550957 CET	80	49711	188.114.97.3	192.168.2.5
Nov 29, 2022 10:34:27.527229071 CET	80	49711	188.114.97.3	192.168.2.5
Nov 29, 2022 10:34:27.581789970 CET	49711	80	192.168.2.5	188.114.97.3
Nov 29, 2022 10:34:27.746809959 CET	80	49711	188.114.97.3	192.168.2.5
Nov 29, 2022 10:34:27.746951103 CET	49711	80	192.168.2.5	188.114.97.3
Nov 29, 2022 10:34:27.747056961 CET	49711	80	192.168.2.5	188.114.97.3
Nov 29, 2022 10:34:27.763880968 CET	80	49711	188.114.97.3	192.168.2.5
Nov 29, 2022 10:34:32.948474884 CET	49713	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:33.073626041 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.073754072 CET	49713	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:33.073966026 CET	49713	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:33.199038029 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.208233118 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.208273888 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.208291054 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.208312035 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.208324909 CET	80	49713	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:33.208365917 CET	49713	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:33.208442926 CET	49713	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:34.135485888 CET	49713	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:35.153863907 CET	49714	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:35.277013063 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.277270079 CET	49714	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:35.314305067 CET	49714	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:35.437031031 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.449829102 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.449894905 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.449937105 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.449982882 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.450016975 CET	80	49714	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:35.450097084 CET	49714	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:35.450154066 CET	49714	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:36.332655907 CET	49714	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.349132061 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.474024057 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.474205017 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.474416971 CET	49715	80	192.168.2.5	192.185.90.105

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:34:37.599165916 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611229897 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611268044 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611294031 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611318111 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611341000 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611363888 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611397982 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611421108 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611470938 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.611489058 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611512899 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611548901 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:37.611562014 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.611613989 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.611634016 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.611891031 CET	49715	80	192.168.2.5	192.185.90.105
Nov 29, 2022 10:34:37.737736940 CET	80	49715	192.185.90.105	192.168.2.5
Nov 29, 2022 10:34:42.668643951 CET	49716	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:42.685606003 CET	80	49716	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:42.685733080 CET	49716	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:42.685957909 CET	49716	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:42.703064919 CET	80	49716	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:43.030292988 CET	80	49716	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:43.030323029 CET	80	49716	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:43.030469894 CET	49716	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:43.030601025 CET	80	49716	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:43.030718088 CET	49716	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:43.692905903 CET	49716	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:44.720374107 CET	49717	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:44.737757921 CET	80	49717	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:44.737936020 CET	49717	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:44.738449097 CET	49717	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:44.755218029 CET	80	49717	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:45.082472086 CET	80	49717	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:45.082529068 CET	80	49717	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:45.082606077 CET	80	49717	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:45.082668066 CET	49717	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:45.082818985 CET	49717	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:45.739542007 CET	49717	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:46.756083965 CET	49719	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:46.773236036 CET	80	49719	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:46.774192095 CET	49719	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:46.780267000 CET	49719	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:46.797194004 CET	80	49719	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:47.155785084 CET	80	49719	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:47.155965090 CET	80	49719	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:47.156471014 CET	49719	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:47.156668901 CET	49719	80	192.168.2.5	172.67.214.243
Nov 29, 2022 10:34:47.173491955 CET	80	49719	172.67.214.243	192.168.2.5
Nov 29, 2022 10:34:52.715010881 CET	49720	80	192.168.2.5	206.83.40.92
Nov 29, 2022 10:34:52.743273973 CET	80	49720	206.83.40.92	192.168.2.5
Nov 29, 2022 10:34:52.743366957 CET	49720	80	192.168.2.5	206.83.40.92
Nov 29, 2022 10:34:52.743576050 CET	49720	80	192.168.2.5	206.83.40.92
Nov 29, 2022 10:34:52.771430969 CET	80	49720	206.83.40.92	192.168.2.5
Nov 29, 2022 10:34:52.781203032 CET	80	49720	206.83.40.92	192.168.2.5
Nov 29, 2022 10:34:52.781259060 CET	80	49720	206.83.40.92	192.168.2.5
Nov 29, 2022 10:34:52.781282902 CET	80	49720	206.83.40.92	192.168.2.5
Nov 29, 2022 10:34:52.781383991 CET	49720	80	192.168.2.5	206.83.40.92

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:34:27.014851093 CET	63446	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:34:27.040199995 CET	53	63446	8.8.8.8	192.168.2.5
Nov 29, 2022 10:34:32.821219921 CET	55039	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:34:32.943109035 CET	53	55039	8.8.8.8	192.168.2.5
Nov 29, 2022 10:34:42.643572092 CET	60975	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:34:42.667421103 CET	53	60975	8.8.8.8	192.168.2.5
Nov 29, 2022 10:34:52.171785116 CET	55068	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:34:52.190450907 CET	53	55068	8.8.8.8	192.168.2.5
Nov 29, 2022 10:35:01.977390051 CET	56682	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:35:02.101298094 CET	53	56682	8.8.8.8	192.168.2.5
Nov 29, 2022 10:35:11.693732977 CET	62659	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:35:11.952652931 CET	53	62659	8.8.8.8	192.168.2.5
Nov 29, 2022 10:35:21.715904951 CET	58581	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:35:21.738689899 CET	53	58581	8.8.8.8	192.168.2.5
Nov 29, 2022 10:35:31.672270060 CET	65513	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:35:32.116449118 CET	53	65513	8.8.8.8	192.168.2.5
Nov 29, 2022 10:35:42.613173008 CET	56687	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:35:42.635181904 CET	53	56687	8.8.8.8	192.168.2.5
Nov 29, 2022 10:35:52.713239908 CET	64419	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:35:52.783279896 CET	53	64419	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:01.994003057 CET	61344	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:02.056188107 CET	53	61344	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:11.792120934 CET	53972	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:12.027338028 CET	53	53972	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:22.629139900 CET	64932	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:23.740036964 CET	64932	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:23.798295975 CET	53	64932	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:23.905383110 CET	53	64932	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:33.592092037 CET	58472	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:33.618837118 CET	53	58472	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:43.376907110 CET	60177	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:43.399647951 CET	53	60177	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:52.984909058 CET	60019	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:53.005125046 CET	53	60019	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:54.015237093 CET	50902	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:54.035623074 CET	53	50902	8.8.8.8	192.168.2.5
Nov 29, 2022 10:36:55.045731068 CET	53823	53	192.168.2.5	8.8.8.8
Nov 29, 2022 10:36:55.074374914 CET	53	53823	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 29, 2022 10:36:23.905508995 CET	192.168.2.5	8.8.8.8	d009	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 10:34:27.014851093 CET	192.168.2.5	8.8.8.8	0x32a7	Standard query (0)	www.oonrreward.xyz	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:32.821219921 CET	192.168.2.5	8.8.8.8	0x1ae6	Standard query (0)	www.gmrsnodes.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:42.643572092 CET	192.168.2.5	8.8.8.8	0xa69f	Standard query (0)	www.dailyheraldresearch.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:52.171785116 CET	192.168.2.5	8.8.8.8	0x1a48	Standard query (0)	www.publickit.website	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:01.977390051 CET	192.168.2.5	8.8.8.8	0xa16d	Standard query (0)	www.lee-perez.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 10:35:11.693732977 CET	192.168.2.5	8.8.8.8	0x3e57	Standard query (0)	www.frwqc.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:21.715904951 CET	192.168.2.5	8.8.8.8	0x7daf	Standard query (0)	www.tommy57.shop	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:31.672270060 CET	192.168.2.5	8.8.8.8	0x2c4a	Standard query (0)	www.700544.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:42.613173008 CET	192.168.2.5	8.8.8.8	0x57e8	Standard query (0)	www.porggiret.site	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:52.713239908 CET	192.168.2.5	8.8.8.8	0x9426	Standard query (0)	www.tobewell.store	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:01.994003057 CET	192.168.2.5	8.8.8.8	0xbe35	Standard query (0)	www.new-thinking.digital	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:11.792120934 CET	192.168.2.5	8.8.8.8	0x2b64	Standard query (0)	www.ybkos.link	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:22.629139900 CET	192.168.2.5	8.8.8.8	0x906e	Standard query (0)	www.bookmygennie.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:23.740036964 CET	192.168.2.5	8.8.8.8	0x906e	Standard query (0)	www.bookmygennie.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:33.592092037 CET	192.168.2.5	8.8.8.8	0x92e2	Standard query (0)	www.amspustaka.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:43.376907110 CET	192.168.2.5	8.8.8.8	0x5112	Standard query (0)	www.spirituallyzen.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:52.984909058 CET	192.168.2.5	8.8.8.8	0x10fd	Standard query (0)	www.davidemarone.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:54.015237093 CET	192.168.2.5	8.8.8.8	0xdf56	Standard query (0)	www.davidemarone.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:55.045731068 CET	192.168.2.5	8.8.8.8	0xa18f	Standard query (0)	www.davidemarone.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
Nov 29, 2022 10:34:27.040199995 CET	8.8.8.8	192.168.2.5	0x32a7	No error (0)	www.oonrreward.xyz		188.114.97.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:27.040199995 CET	8.8.8.8	192.168.2.5	0x32a7	No error (0)	www.oonrreward.xyz		188.114.96.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:32.943109035 CET	8.8.8.8	192.168.2.5	0x1ae6	No error (0)	www.gmrsnodes.com	gmrsnodes.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:34:32.943109035 CET	8.8.8.8	192.168.2.5	0x1ae6	No error (0)	gmrsnodes.com		192.185.90.105	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:42.667421103 CET	8.8.8.8	192.168.2.5	0xa69f	No error (0)	www.dailyheraldresearch.com		172.67.214.243	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:42.667421103 CET	8.8.8.8	192.168.2.5	0xa69f	No error (0)	www.dailyheraldresearch.com		104.21.83.59	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:34:52.190450907 CET	8.8.8.8	192.168.2.5	0x1a48	No error (0)	www.publickit.website	publickit.website		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:34:52.190450907 CET	8.8.8.8	192.168.2.5	0x1a48	No error (0)	publickit.website		206.83.40.92	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:02.101298094 CET	8.8.8.8	192.168.2.5	0xa16d	No error (0)	www.lee-perez.com		216.40.34.41	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:11.952652931 CET	8.8.8.8	192.168.2.5	0x3e57	No error (0)	www.frwqc.com		38.40.166.195	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:21.738689899 CET	8.8.8.8	192.168.2.5	0x7daf	No error (0)	www.tommy57.shop		74.208.236.65	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:32.116449118 CET	8.8.8.8	192.168.2.5	0x2c4a	No error (0)	www.700544.com	pp.3105.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:35:32.116449118 CET	8.8.8.8	192.168.2.5	0x2c4a	No error (0)	pp.3105.net		93.179.127.27	A (IP address)	IN (0x0001)	false

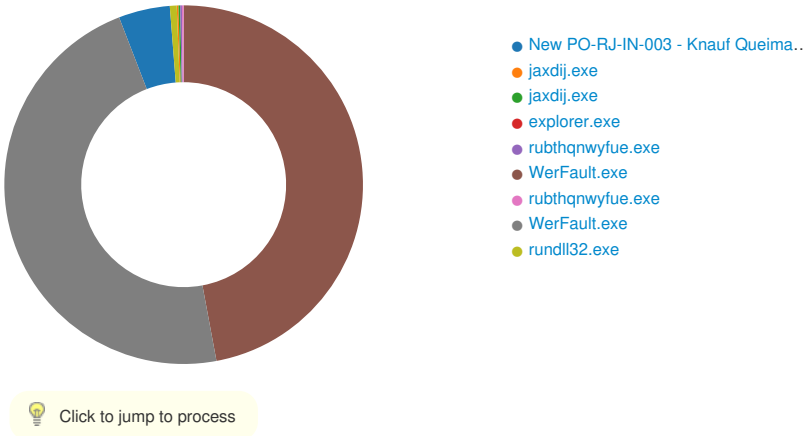
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 10:35:32.116449118 CET	8.8.8.8	192.168.2.5	0x2c4a	No error (0)	pp.3105.net		93.179.126.57	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:32.116449118 CET	8.8.8.8	192.168.2.5	0x2c4a	No error (0)	pp.3105.net		93.179.126.25	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:42.635181904 CET	8.8.8.8	192.168.2.5	0x57e8	No error (0)	www.porggiret.site		198.54.121.81	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:35:52.783279896 CET	8.8.8.8	192.168.2.5	0x9426	No error (0)	www.tobewell.store	tobewell.store		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:35:52.783279896 CET	8.8.8.8	192.168.2.5	0x9426	No error (0)	tobewell.store		178.208.83.20	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:02.056188107 CET	8.8.8.8	192.168.2.5	0xbe35	No error (0)	www.new-thinking.digital		62.233.121.61	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:12.027338028 CET	8.8.8.8	192.168.2.5	0x2b64	No error (0)	www.ybkos.link		107.148.15.81	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:23.798295975 CET	8.8.8.8	192.168.2.5	0x906e	No error (0)	www.bookmygennie.com		38.163.214.169	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:23.905383110 CET	8.8.8.8	192.168.2.5	0x906e	No error (0)	www.bookmygennie.com		38.163.214.169	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:33.618837118 CET	8.8.8.8	192.168.2.5	0x92e2	No error (0)	www.amspustaka.com	amspustaka.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:36:33.618837118 CET	8.8.8.8	192.168.2.5	0x92e2	No error (0)	amspustaka.com		23.111.12.177	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:43.399647951 CET	8.8.8.8	192.168.2.5	0x5112	No error (0)	www.spirituallyzen.com		74.208.236.214	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:53.005125046 CET	8.8.8.8	192.168.2.5	0x10fd	Name error (3)	www.davidemarone.com	none	none	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:54.035623074 CET	8.8.8.8	192.168.2.5	0xdf56	Name error (3)	www.davidemarone.com	none	none	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:36:55.074374914 CET	8.8.8.8	192.168.2.5	0xa18f	Name error (3)	www.davidemarone.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.oonrreward.xyz
- www.gmrsnodes.com
- www.dailyheraldresearch.com
- www.publickit.website
- www.lee-perez.com
- www.frwqc.com
- www.tommy57.shop
- www.700544.com
- www.porggiret.site
- www.tobewell.store
- www.new-thinking.digital
- www.ybkos.link
- www.bookmygennie.com
- www.amspustaka.com
- www.spirituallyzen.com

Statistics

Behavior



System Behavior

Analysis Process: New PO-RJ-IN-003 - Knauf Queimados.exe PID: **748**, Parent PID: **3324**

General

Target ID:	0
Start time:	10:33:03
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New PO-RJ-IN-003 - Knauf Queimados.exe
Imagebase:	0x400000
File size:	405670 bytes
MD5 hash:	244FC9610F75225AA3DC09958195BEB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: jaxdij.exe PID: **1572**, Parent PID: **748**

General

Target ID:	1
Start time:	10:33:03
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\jaxdij.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\Local\Temp\uqnwrddys.k
Imagebase:	0x240000
File size:	147968 bytes
MD5 hash:	2DD6C8B13AE7D028B0047435FF0DCB8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 12%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\uqnwrddys.k	unknown	7706	success or wait	1	241A1D	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: jaxdij.exe PID: **5360**, Parent PID: **1572**

General

Target ID:	2
Start time:	10:33:04

Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\jaxdij.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\Local\Temp\uqnwrddys.k
Imagebase:	0x240000
File size:	147968 bytes
MD5 hash:	2DD6C8B13AE7D028B0047435FF0DCB8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.417309274.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.417309274.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.417309274.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.417309274.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.417458366.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.417458366.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.417458366.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.417458366.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.415905710.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.415905710.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.415905710.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.415905710.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41DFAE	NtReadFile

Analysis Process: explorer.exe PID: **3324**, Parent PID: **5360**

General

Target ID:	3
Start time:	10:33:10
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.383481318.000000001091F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.383481318.000000001091F000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.383481318.000000001091F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.383481318.000000001091F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: rubthqnwyfue.exe PID: **5040**, Parent PID: **3324**

General

Target ID:	4
Start time:	10:33:15
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe" "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\L
Imagebase:	0xb90000
File size:	147968 bytes
MD5 hash:	2DD6C8B13AE7D028B0047435FF0DCB8A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 12%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4294967295	object type mismatch	1	B91A1D	ReadFile

Analysis Process: WerFault.exe PID: **2912**, Parent PID: **5040**

General

Target ID:	7
Start time:	10:33:19
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5040 -s 476
Imagebase:	0xe70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE41717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A3.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_0b3f82dd	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_0b3f82dd\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A3.tmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A3.tmp.xml	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D0.tmp.csv	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER496.tmp.txt	success or wait	1	6CE3497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 71 50 fd 63 fd 05 12 00 00 00 00 00	MDMP qPc	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	6052	6	00 00 00 00 00 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.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 17 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 6b 50 fd 63 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 20 00 00 0d 00 00 00 00 00 00 00 01 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 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	UBGenuineIntelWTkPc Pacific Standard TimePacific Daylight Time	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	6976	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 fd fd fd fd 00 fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 14 fd fd 00 26 1a fd 00 23 00 00 00 02 02 01 00 68 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++m&#h+	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	1620	168	fd 11 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 26 1a fd 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 40 1b 00 00	&@	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	9840	20	0f 00 00 00 fd fd 00 00 00 00 00 14 14 00 00 64 27 00 00	d'	success or wait	15	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	10084	5140	fd fd 0f 77 fd 1a fd 74 fd fd fd fd 20 fd 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 01 00 00 fd 00 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wt $m	success or wait	14	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	28780	4096	fd fd fd 00 00 00 fd 00 00 fd fd 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 20 6e 00 00 00 00 00 fd 13 00 00 30 11 00 00 00 00 00 00 00 00 00 00 00 fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 08 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	n0mpw	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	7692	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 00 fd fd 0f 77 23 00 00 00 16 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#+	success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	1888	48	30 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 6e 00 00 00 00 00 fd fd fd 00 00 00 00 00 18 03 00 00 fd 45 00 00 fd 02 00 00 fd 23 00 00	0 nE#	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	1948	4	20 00 00 00		success or wait	32	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	6058	38	20 00 00 00 72 00 75 00 62 00 74 00 68 00 71 00 6e 00 77 00 79 00 66 00 75 00 65 00 2e 00 65 00 78 00 65 00 00 00	rubthqnwyfue.exe	success or wait	32	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	5300	752	00 00 fd 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 28 1b 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 20 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 58 74 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 5e fd 03 00 00 00 00 00 73 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 18 1b 00 00 00 00 00 6b fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 61 1f 05 00 00 00 00	v`A!-a(BB?#@AZb FXt^sk@a	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	32876	7256	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 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF75.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 0d 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 70 26 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 20 13 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 20 15 00 00 16 00 00 00 fd 00 00 00 0c 17 00 00	p&T8T	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5040</Pid>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1002	78	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 62 00 74 00 68 00 71 00 6e 00 77 00 79 00 66 00 75 00 65 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>rubthqnwyfue.exe</ImageName>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1080	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1084	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1088	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 32 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>00000002</CmdLineSignature>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1178	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1182	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1186	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6279</Uptime>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1236	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1326	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1386	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1440	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 36 00 30 00 39 00 33 00 32 00 30 00 39 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>60932096</PeakVirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1536	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 36 00 30 00 39 00 32 00 33 00 39 00 30 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>60923904</VirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1616	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 37 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2722</PageFaultCount>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1700	98	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 31 00 30 00 35 00 35 00 35 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10555392</PeakWorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1798	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1802	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1808	82	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 31 00 30 00 35 00 35 00 35 00 33 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10555392</WorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1890	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1894	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	1900	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 30 00 38 00 35 00 39 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>108592</QuotaPeakPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2014	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2018	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2024	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 30 00 38 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>108024</QuotaPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2122	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2126	2	09 00		success or wait	3	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2132	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 34 00 39 00 38 00 30 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>49808</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2256	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2260	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2266	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 34 00 39 00 35 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>49536</QuotaNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2374	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2378	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2384	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 37 00 35 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5357568</PagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2460	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2464	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2470	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 36 00 35 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5365760</PeakPagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2572	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 37 00 35 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5357568</PrivateUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2644	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2648	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2652	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2698	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2702	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2706	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2736	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2740	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2746	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2786	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2790	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2798	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2828	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2832	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2840	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 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>explorer.exe</ImageName>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2910	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2914	2	09 00		success or wait	4	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	2922	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3012	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3016	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3024	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 32 00 35 00 35 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6225542</Uptime>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3072	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3076	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3084	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3162	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3166	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3174	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3238	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3282	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3286	2	09 00		success or wait	5	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3296	90	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</PeakVirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3386	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3390	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3400	74	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</VirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3474	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3478	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3488	76	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 36 00 35 00 31 00 36 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>65166</PageFaultCount>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3578	100	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 31 00 33 00 39 00 32 00 31 00 38 00 39 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>139218944</PeakWorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3692	84	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 31 00 33 00 33 00 33 00 38 00 32 00 31 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>133382144</WorkingSetSize>	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3776	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3780	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3790	116	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 31 00 37 00 33 00 30 00 38 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 50 00 61 00 67 00 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>11730 88</QuotaPeakPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	3920	100	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 31 00 33 00 38 00 35 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 >1138552</ QuotaPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4020	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4024	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4034	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 39 00 31 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4158	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4162	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4172	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 38 00 33 00 32 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>83200< /QuotaNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4280	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4284	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4294	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 36 00 31 00 39 00 34 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4161945 6</PagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4372	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4376	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4386	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 30 00 31 00 37 00 34 00 30 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>48 017408</P eakPagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4480	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4484	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4494	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 36 00 31 00 39 00 34 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4161945 6</PrivateUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4568	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4572	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4580	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4636	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4678	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4682	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4686	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4724	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4766	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4770	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4772	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4810	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4814	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4818	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4880	4	0d 00 0a 00		success or wait	8	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4884	2	09 00		success or wait	16	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	4888	82	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 62 00 74 00 68 00 71 00 6e 00 77 00 79 00 66 00 75 00 65 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>rubthqnwyfue.exe</Parameter0>	success or wait	8	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5500	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5504	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5506	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5546	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5550	2	09 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5552	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5590	4	0d 00 0a 00		success or wait	6	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5594	2	09 00		success or wait	12	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	5598	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6152	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6156	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6158	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6198	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6202	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6204	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6242	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6246	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6250	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6352	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 63 00 6a 00 75 00 66 00 78 00 65 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>cjufxe, Inc.</SystemManufacturer>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6458	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6462	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6466	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 63 00 6a 00 75 00 66 00 78 00 65 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>cjufxe7,1</SystemProductName>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6562	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6566	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6570	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6690	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6694	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6698	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 30 00 38 00 32 00 38 00 32 00 39 00 34 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>1608282947</OSInstallDate>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6780	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6784	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6788	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6890	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6894	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6898	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6966	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6970	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	6972	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7012	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7016	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7018	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7052	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7056	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7060	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7156	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7160	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7162	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	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7198	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7202	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7204	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7228	4	0d 00 0a 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7232	2	09 00		success or wait	6	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7236	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7482	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7486	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7488	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7514	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7518	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7520	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 32 00 2d 00 31 00 31 00 2d 00 32 00 39 00 54 00 31 00 38 00 3a 00 33 00 33 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-29T18:33:21Z">	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7620	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7624	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7628	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 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 30 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 30 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 35 00 30 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="306" PID="5040" UptimeMS="500" TimeSinceCreationMS="500" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7886	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7890	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7894	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7920	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7958	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7962	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	7964	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8002	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8006	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8010	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 31 00 62 00 33 00 34 00 32 00 30 00 32 00 2d 00 34 00 34 00 62 00 35 00 2d 00 34 00 64 00 62 00 37 00 2d 00 39 00 66 00 62 00 37 00 2d 00 38 00 63 00 30 00 61 00 30 00 63 00 30 00 65 00 61 00 32 00 39 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>01b34202-44b5-4db7-9fb7-8c0a0c0ea296</Guid>	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8108	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8112	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8116	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 32 00 2d 00 31 00 31 00 2d 00 32 00 39 00 54 00 31 00 38 00 3a 00 33 00 33 00 3a 00 32 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>2022-11-29T18:33 :21Z</CreationTime>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8214	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8218	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8220	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8260	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER206.tmp.WERInternalMetadata.xml	8264	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A3.tmp.xml	0	4577	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_0b3f82dd\Report.wer	0	2	fd fd		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_0b3f82dd\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	157	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_0b3f82dd\Report.wer	10340	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 31 00 30 00 39 00 36 00 37 00 32 00 32 00 39 00 31 00	MetadataHash=1109672291	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

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: rubthqnwyfue.exe PID: **6040**, Parent PID: **3324**

General

Target ID:	8
Start time:	10:33:24
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\fqkyib\rubthqnwyfue.exe" "C:\Users\user\AppData\Local\Temp\jaxdij.exe" C:\Users\user\AppData\L
Imagebase:	0xb90000
File size:	147968 bytes
MD5 hash:	2DD6C8B13AE7D028B0047435FF0DCB8A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4294967295	object type mismatch	1	B91A1D	ReadFile

Analysis Process: WerFault.exe PID: **5420**, Parent PID: **6040**

General

Target ID:	10
Start time:	10:33:26
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 444
Imagebase:	0xe70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE41717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1810.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1810.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_15731f22	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_15731f22\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE3497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1810.tmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1810.tmp.xml	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER184E.tmp.csv	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A14.tmp.txt	success or wait	1	6CE3497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 77 50 fd 63 fd 05 12 00 00 00 00 00	MDMP wPc	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	5944	6	00 00 00 00 00 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.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 38 17 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 74 50 fd 63 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 20 00 00 0d 00 00 00 00 00 00 00 01 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	UB8GenuineIntelWTtPcPacific Standard TimePacific Daylight Time	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	6840	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 fd fd fd fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 64 fd 13 01 26 1a fd 00 23 00 00 00 06 02 01 00 fd fd 13 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++d&#+	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	1620	168	fd 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 26 1a fd 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1a 00 00	&	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	9704	20	0f 00 00 00 20 31 3d 01 00 00 00 00 04 00 00 00 fd 26 00 00	1=&	success or wait	15	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	9948	4	28 fd 5c 01	(\	success or wait	14	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	30200	1000	fd fd 0f 77 fd fd 0d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 6c 01 78 fd 6c 01 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 30 3d 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 3d 01 00 00 00 00 00 00 00 00 fd 32 3d 01 00 00 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 02 fd 00 20 fd 5c 01 20 31 3d 01 28 fd 5c 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwlxl@w@w0==2=T \ 1= (\	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	7556	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 13 01 fd fd 0f 77 23 00 00 00 12 02 00 00 40 fd 13 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#@+	success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	1888	48	1c 0b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 18 fd 6c 01 00 00 00 00 fd 03 00 00 fd 75 00 00 fd 02 00 00 1c 23 00 00	lu#	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	1948	4	1f 00 00 00		success or wait	31	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	5950	38	20 00 00 00 72 00 75 00 62 00 74 00 68 00 71 00 6e 00 77 00 79 00 66 00 75 00 65 00 2e 00 65 00 78 00 65 00 00 00	rubthqnwyfue.exe	success or wait	31	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	5192	752	00 00 fd 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1a 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 fd 74 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 1d fd 03 00 00 00 00 00 7d fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 23 1d 1b 00 00 00 00 00 1d fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 61 1f 05 00 00 00 00	v`A!-aBB? #@AZbPFt}#@a	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	31200	6924	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1493.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 18 0d 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 25 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 11 00 00 0c fd 00 00 15 00 00 00 fd 01 00 00 fd 14 00 00 16 00 00 00 fd 00 00 00 fd 16 00 00	%T8T	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6040</Pid>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1002	78	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 62 00 74 00 68 00 71 00 6e 00 77 00 79 00 66 00 75 00 65 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>rubthqnwyfue.exe</ImageName>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1080	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1084	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1088	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 32 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>00000002</CmdLineSignature>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1178	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1182	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1186	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3084</Uptime>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1236	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1326	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1386	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1440	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 36 00 30 00 32 00 37 00 32 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>60272640</PeakVirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1536	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 36 00 30 00 32 00 36 00 34 00 34 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>60264448</VirtualSize>	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1616	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 36 00 31 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>2619</PageFaultCount>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1700	98	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 31 00 30 00 31 00 36 00 36 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10166272</PeakWorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1798	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1802	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1808	82	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 31 00 30 00 31 00 36 00 36 00 32 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10166272</WorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1890	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1894	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	1900	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 30 00 37 00 33 00 32 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>107320</QuotaPeakPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2014	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2018	2	09 00		success or wait	3	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2024	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 30 00 36 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>106752</QuotaPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2122	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2126	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2132	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 34 00 39 00 34 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>49464</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2256	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2260	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2266	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 34 00 39 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>49112</QuotaNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2374	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2378	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2384	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 30 00 38 00 34 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5308416</PagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2460	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2464	2	09 00		success or wait	3	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2470	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 31 00 36 00 36 00 30 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>53 16608</Pe akPagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2572	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 30 00 38 00 34 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5308416 </PrivateUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2644	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2648	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2652	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2698	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2702	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2706	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2736	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2740	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2746	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2786	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2790	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2798	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2828	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2832	2	09 00		success or wait	4	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2840	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 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>explorer.exe</ImageName>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2910	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2914	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	2922	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3012	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3016	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3024	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 33 00 31 00 30 00 30 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6231001</Uptime>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3072	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3076	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3084	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3162	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3166	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3174	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3238	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	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3282	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3286	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3296	90	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</PeakVirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3386	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3390	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3400	74	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</VirtualSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3474	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3478	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3488	76	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 36 00 36 00 34 00 32 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>66420</PageFaultCount>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3578	100	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 31 00 33 00 39 00 32 00 31 00 38 00 39 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>139218944</PeakWorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3692	84	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 31 00 33 00 36 00 37 00 30 00 34 00 30 00 30 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>136704000</WorkingSetSize>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3776	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3780	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3790	116	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 31 00 37 00 33 00 30 00 38 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 50 00 61 00 67 00 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>1173088</QuotaPeakPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	3920	100	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 31 00 32 00 38 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1128888</QuotaPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4020	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4024	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4034	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 39 00 31 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>91984</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4158	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4162	2	09 00		success or wait	5	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4172	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 38 00 32 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>82384</QuotaNonPagedPoolUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4280	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4284	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4294	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 35 00 32 00 31 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>41521152</PagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4372	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4376	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4386	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 30 00 31 00 37 00 34 00 30 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>48017408</PeakPagefileUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4480	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4484	2	09 00		success or wait	5	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4494	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 35 00 32 00 31 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>415211 52</PrivateUsage>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4568	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4572	2	09 00		success or wait	4	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4580	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4636	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4678	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4682	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4686	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4724	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4766	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4770	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4772	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4810	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4814	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4818	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4880	4	0d 00 0a 00		success or wait	8	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4884	2	09 00		success or wait	16	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	4888	82	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 62 00 74 00 68 00 71 00 6e 00 77 00 79 00 66 00 75 00 65 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>rubthqnwyfue.exe</Parameter0>	success or wait	8	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5500	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5504	2	09 00		success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5506	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5546	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5550	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5552	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5590	4	0d 00 0a 00		success or wait	6	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5594	2	09 00		success or wait	12	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	5598	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6152	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6156	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6158	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6198	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6202	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6204	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6242	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6246	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6250	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6352	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 63 00 6a 00 75 00 66 00 78 00 65 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>cjufxe, Inc.</SystemManufacturer>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6458	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6462	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6466	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 63 00 6a 00 75 00 66 00 78 00 65 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>cjufxe7,1</SystemProductName>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6562	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6566	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6570	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6690	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6694	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6698	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 30 00 38 00 32 00 38 00 32 00 39 00 34 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>1608282947</OSInstallDate>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6780	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6784	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6788	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6890	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6894	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6898	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6966	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6970	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	6972	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7012	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7016	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7018	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7052	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7056	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7060	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7156	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7160	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7162	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	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7198	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7202	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7204	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7228	4	0d 00 0a 00		success or wait	3	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7232	2	09 00		success or wait	6	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7236	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7494	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7498	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7500	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7526	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7530	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7532	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 32 00 2d 00 31 00 31 00 2d 00 32 00 39 00 54 00 31 00 38 00 3a 00 33 00 33 00 3a 00 32 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-29T18:33:27Z">	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7632	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7636	2	09 00		success or wait	2	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7640	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 31 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 30 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 38 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="311" PID="6040" UptimeMS="687" TimeSinceCreationMS="687" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7906	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7932	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	7976	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8014	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8018	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8022	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 34 00 37 00 38 00 31 00 37 00 35 00 33 00 2d 00 39 00 39 00 39 00 62 00 2d 00 34 00 32 00 31 00 33 00 2d 00 61 00 64 00 33 00 35 00 2d 00 38 00 37 00 35 00 32 00 61 00 65 00 64 00 61 00 63 00 32 00 34 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>04781753-999b-4213-ad35-8752aedac24d</Guid>	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8120	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8124	2	09 00		success or wait	2	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8128	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 32 00 2d 00 31 00 31 00 2d 00 32 00 39 00 54 00 31 00 38 00 3a 00 33 00 33 00 3a 00 32 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-29T18:33 :27Z</CreationTime>	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8232	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8272	4	0d 00 0a 00		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1753.tmp.WERInternalMetadata.xml	8276	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	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1810.tmp.xml	0	4577	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_15731f22\Report.wer	0	2	fd fd		success or wait	1	6CE3497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_15731f22\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	156	6CE3497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rubthqnwyfue.exe_1078f5d9a12c4fe091b0b1b063f9270e1879244_c652c34e_15731f22\Report.wer	10238	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 30 00 31 00 37 00 37 00 30 00 37 00 35 00 35 00	MetadataHash=-1501770755	success or wait	1	6CE3497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5412**, Parent PID: **3324**

General

Target ID:	11
Start time:	10:33:54
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x380000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.821380016.0000000000500000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.822152428.0000000004480000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.822152428.0000000004480000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.822152428.0000000004480000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.822152428.0000000004480000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.821985368.0000000002CC0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.821985368.0000000002CC0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.821985368.0000000002CC0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.821985368.0000000002CC0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\456b6ELMQ	object name not found	1	2CDC8A7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\456b6ELMQ	sharing violation	1	2CDC8A7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\456b6ELMQ	sharing violation	1	2CDC8A7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2CDC877	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly