



ID: 750456
Sample Name: kOiaWLNKXpjayWeM.dll
Cookbook: default.jbs
Time: 03:31:51
Date: 21/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report kOiaWLNKXpjayWeM.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 6
Boot Survival 6
Hooking and other Techniques for Hiding and Protection 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4\Report.wer 14
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813\Report.wer 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp.xml 16
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 18
Sections 19
Resources 19
Imports 19
Exports 20
Possible Origin 20
Network Behavior 21
Snort IDS Alerts 21
TCP Packets 21
HTTP Request Dependency Graph 21
Statistics 21
Behavior 21

System Behavior 22
Analysis Process: loaddll64.exePID: 6112, Parent PID: 3452 22
General 22
File Activities 22
Analysis Process: conhost.exePID: 6096, Parent PID: 6112 22
General 22
Analysis Process: cmd.exePID: 6044, Parent PID: 6112 23
General 23
File Activities 23
Analysis Process: regsvr32.exePID: 6076, Parent PID: 6112 23
General 23
File Activities 23
File Deleted 23
Analysis Process: rundll32.exePID: 6128, Parent PID: 6044 24
General 24
Analysis Process: rundll32.exePID: 2424, Parent PID: 6112 24
General 24
Analysis Process: regsvr32.exePID: 5252, Parent PID: 6076 24
General 24
Registry Activities 25
Key Value Created 25
Analysis Process: rundll32.exePID: 5228, Parent PID: 6112 25
General 25
File Activities 25
Analysis Process: WerFault.exePID: 5204, Parent PID: 6128 25
General 25
File Activities 26
File Created 26
File Deleted 26
File Written 26
Registry Activities 49
Key Created 49
Key Value Created 49
Key Value Modified 50
Analysis Process: WerFault.exePID: 3332, Parent PID: 2424 50
General 50
File Activities 50
File Created 50
File Deleted 51
File Written 51
Registry Activities 74
Key Created 74
Analysis Process: rundll32.exePID: 1788, Parent PID: 6112 74
General 74
File Activities 75
Analysis Process: regsvr32.exePID: 6128, Parent PID: 3452 75
General 75
File Activities 75
Analysis Process: regsvr32.exePID: 5288, Parent PID: 6128 75
General 75
Disassembly 76

Copyright Joe Security LLC 2022

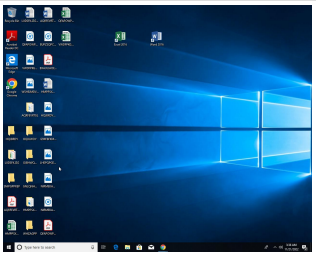
Windows Analysis Report

kOiaWLNKXpjayWeM.dll

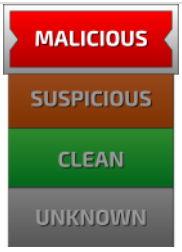
Overview

General Information

Sample Name:	kOiaWLNKXpjayWeM.dll
Analysis ID:	750456
MD5:	b7d93d2b47d142.
SHA1:	9310b16c2d7f91..
SHA256:	139c1faa496ae6..
Infos:	



Detection



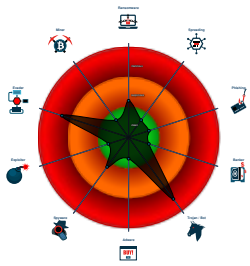
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Creates an autostart registry key po…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fol…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6112 cmdline: loaddll64.exe "C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 6096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6044 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6128 cmdline: rundll32.exe "C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 5204 cmdline: C:\Windows\system32\WerFault.exe -u -p 6128 -s 480 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 6076 cmdline: regsvr32.exe /s C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5252 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\WVVZhuligM\KuLiEStgIluewHbC.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 2424 cmdline: rundll32.exe C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll,?AddArrayString@JKDefragLib@@QEAAPEAPEA_WPEAPEA_WPEA_W@Z MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 3332 cmdline: C:\Windows\system32\WerFault.exe -u -p 2424 -s 472 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 5228 cmdline: rundll32.exe C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll,?CallShowStatus@JKDefragLib@@QEAAXPEAUDefragDataStruct@@HH@Z MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1788 cmdline: rundll32.exe C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll,?ColorizeItem@JKDefragLib@@QEAAXPEAUDefragDataStruct@@PEAUItemStruct@@_K2H@Z MD5: 73C519F050C20580F8A62C849D49215A)
- regsvr32.exe (PID: 6128 cmdline: C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\WVVZhuligM\KuLiEStgIluewHbC.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5288 cmdline: C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\WrWLj\BwssvzQrG.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "218.38.121.17:443",
    "186.250.48.5:443",
    "80.211.107.116:8080",
    "174.138.33.49:7080",
    "165.22.254.236:8080",
    "185.148.169.10:8080",
    "62.171.178.147:8080",
    "128.199.217.206:443",
    "210.57.209.142:8080",
    "36.67.23.59:443",
    "160.16.143.191:8080",
    "128.199.242.164:8080",
    "178.238.225.252:8080",
    "118.98.72.86:443",
    "202.134.4.210:7080",
    "82.98.180.154:7080",
    "54.37.228.122:443",
    "64.227.55.231:8080",
    "195.77.239.39:8080",
    "103.254.12.236:7080",
    "103.85.95.4:8080",
    "178.62.112.199:8080",
    "83.229.80.93:8080",
    "114.79.130.68:443",
    "51.75.33.122:443",
    "139.196.72.155:8080",
    "188.165.79.151:443",
    "190.145.8.4:443",
    "196.44.98.190:8080",
    "198.199.70.22:8080",
    "103.56.149.105:8080",
    "104.244.79.94:443",
    "87.106.97.83:7080",
    "103.71.99.57:8080",
    "46.101.98.60:8080",
    "103.126.216.86:443",
    "103.224.241.74:8080",
    "37.44.244.177:8080",
    "85.214.67.203:8080",
    "202.28.34.99:8080",
    "175.126.176.79:8080",
    "85.25.120.45:8080",
    "93.104.209.107:8080",
    "103.41.204.169:8080",
    "78.47.204.80:443",
    "139.59.80.108:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0Hbtn0QADAJI=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWGLt60QACAIg="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.253014513.0000022AB0991000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.254435708.0000000002401000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.253546936.0000021CE85C1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000016.00000002.371644938.0000000002A00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.254242832.0000000000B00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.21ce8590000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.21ce8590000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.b00000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.0.rundll32.exe.21ce8590000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.22ab0780000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 13 - Source IP: 192.168.2.3 - Destination IP: 218.38.121.17

Timestamp:	192.168.2.3218.38.121.17497144432404324 11/21/22-03:33:25.830611
SID:	2404324
Source Port:	49714
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

Copyright Joe Security LLC 2022

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

Stealing of Sensitive Information

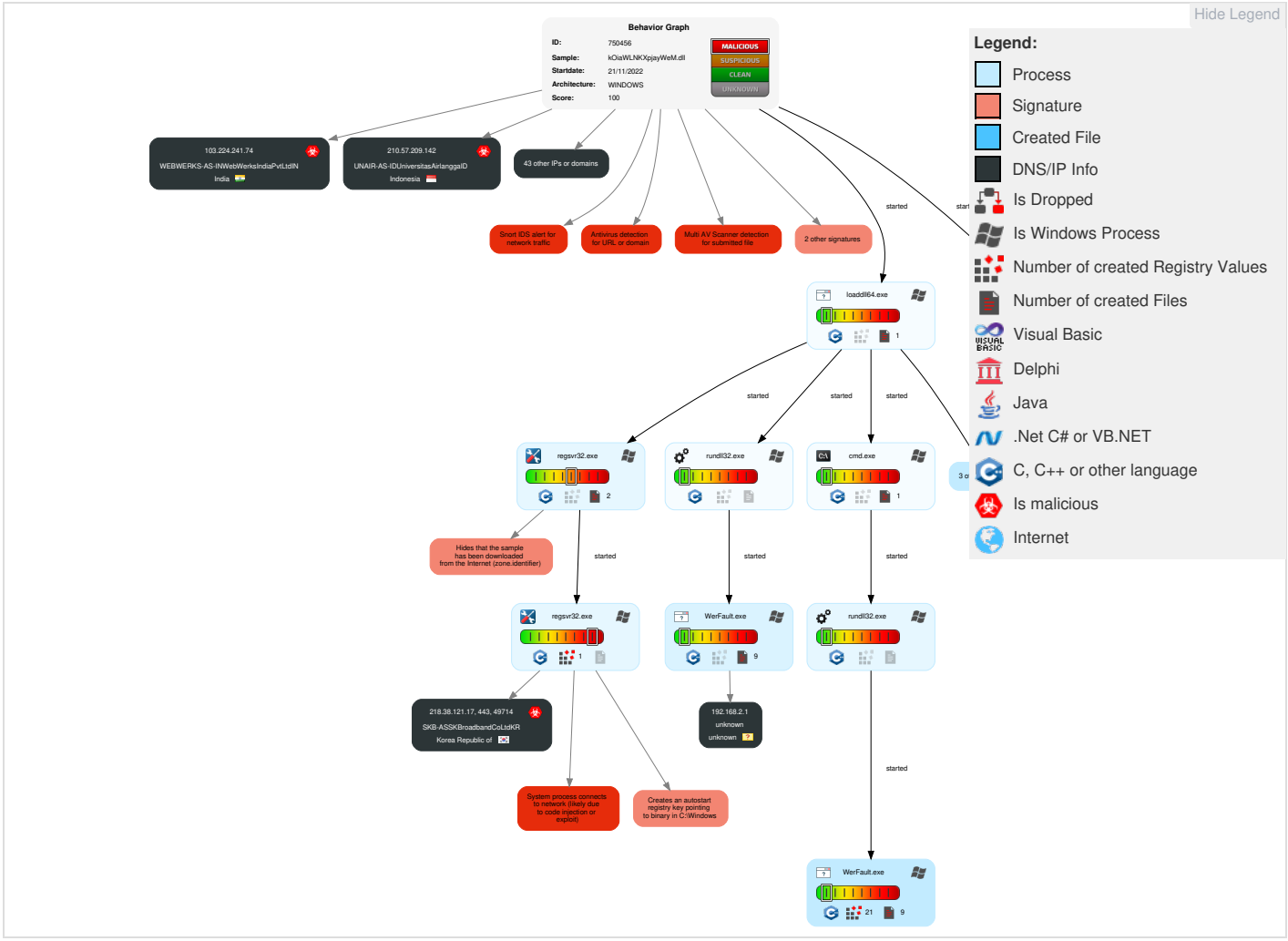


Yara detected Emotet

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	Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	2 1 Masquerading	OS Credential Dumping	1 2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 1 1 Process Injection	2 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 1 1 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	3 File and Directory 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	2 Obfuscated Files or Information	DCSync	1 6 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Regsvr32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 File Deletion	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

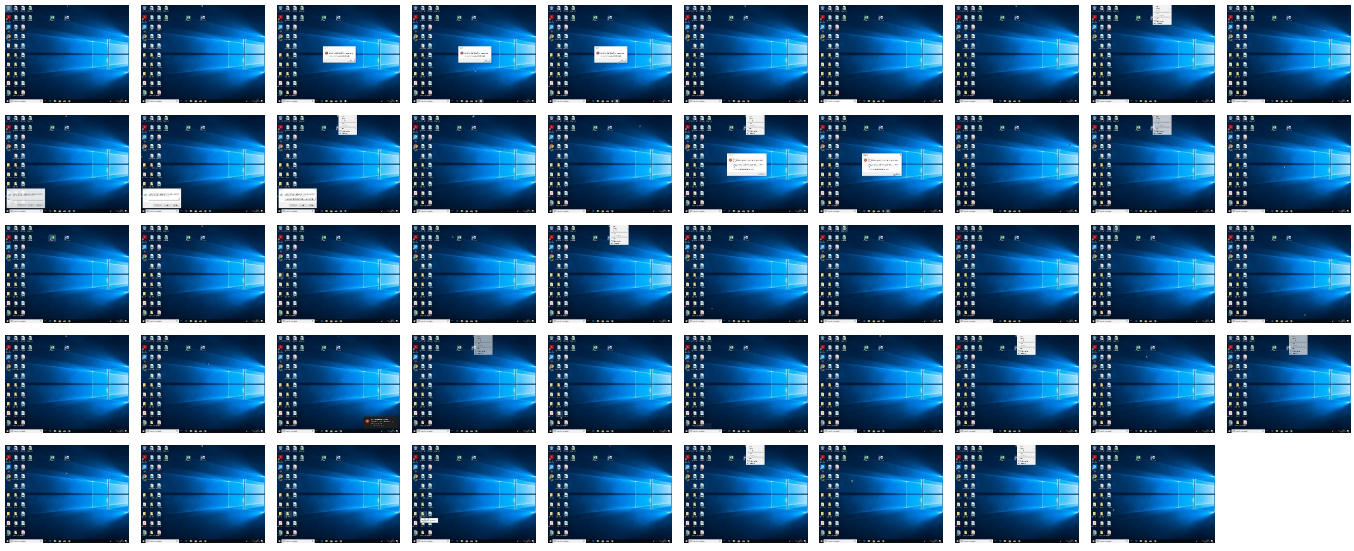
Behavior Graph



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
kOiaWLNKXpjayWeM.dll	88%	ReversingLabs	Win64.Trojan.Emotet	
kOiaWLNKXpjayWeM.dll	73%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.22ab0780000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.b00000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.0.rundll32.exe.21ce8590000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.0.rundll32.exe.21ce8590000.3.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.21ce8590000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.22ab0780000.3.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.22ab0780000.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
22.2.regsvr32.exe.2a00000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.2990000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://218.38.121.17/	0%	URL Reputation	safe	
http://https://218.38.121.17/$	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://218.38.121.17/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://218.38.121.17/$	regsvr32.exe, 00000008.00000002.7676070733.0000000000F14000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.165.79.151	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
160.16.143.191	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
186.250.48.5	unknown	Brazil		262807	RedfoxTelecomunicacoesLtdaBR	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
82.98.180.154	unknown	Spain		42612	DINAHOSTING-ASES	true
114.79.130.68	unknown	India		45769	DVOIS-IND-VoisBroadbandPvtLtdIN	true

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
80.211.107.116	unknown	Italy		31034	ARUBA-ASNIT	true
54.37.228.122	unknown	France		16276	OVHFR	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
218.38.121.17	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
185.148.169.10	unknown	Germany		44780	EVERSCALE-ASDE	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
51.75.33.122	unknown	France		16276	OVHFR	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	750456
Start date and time:	2022-11-21 03:31:51 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kOiaWLNKXpjayWeM.dll
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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@21/8@0/47
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 90% (good quality ratio 84.4%) • Quality average: 74.9% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 20.189.173.21
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, onedsblobprdwus16.westus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:33:03	API Interceptor	2x Sleep call for process: WerFault.exe modified
03:33:28	API Interceptor	1x Sleep call for process: regsvr32.exe modified
03:33:30	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run KuLiEStglluewHbC.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\WVVZhuligM\KuLiEStglluewHbC.dll"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.872078121730829
Encrypted:	false
SSDEEP:	192:940idJK+HOiQCwej1hgc/u7sGS274ltZ:rijK2OVCwejH/u7sGX4ltZ
MD5:	0B151449235445704F036E71D0B36121
SHA1:	B9532A6B689DBBD101DB151FAEEBB0146969F3EC
SHA-256:	1854F3636E6C08507C14FB1D5A4FAE2F3B84C51F775B761F17A1FAB51DB52C4E
SHA-512:	5DB4AE49282BA891FB7FCA08913FCBA872F9CC725E9DD753D165FF544A137251E79C05E28BF19B06A63FE86B0CC7FFB841AD9D58232E485874F6216211C0986
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.3.5.0.3.9.6.9.8.7.1.9.8.8.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.3.5.0.3.9.7.0.8.7.2.0.0.2.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.f.e.9.d.a.1.2.-.5.a.f.5.-.4.5.a.c.-.a.5.4.d.-.1.6.0.9.6.9.e.8.b.1.3.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.8.8.a.3.9.1.2.-.6.0.0.c.-.4.4.c.4.-.a.3.2.9.-.d.a.6.1.a.3.4.8.1.5.0.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.k.O.i.a.W.L.N.K.X.p.j.a.y.W.e.M...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.9.7.8.-.0.0.0.1.-.0.0.1.f.-.7.3.9.a.-.9.e.f.9.9.c.f.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8721527397559001
Encrypted:	false
SSDEEP:	192:/TiuJKeHOiQCwejQh/c/u7sGS274ltZy:biQKWOVCwej3/u7sGX4ltZ
MD5:	89FB0C3122C98458BC77F378EE060B78
SHA1:	5608AFA8320715CB8CECB3D19B4DBED117EE9D3D
SHA-256:	1FB6A0DB37151B85B9A3886768CC49824A9089ACA1126845D28AD56E56B4C8E1
SHA-512:	697CB0AB09C775EE8D2425D2635961DA13EF4EC7EBF12C95575131EEA2276A26D4B2075264BB60053B98DCBC1AAE4FB19A645000165F80D84B5901D2092611F
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.3.5.0.3.9.6.9.3.0.7.7.1.8.9.....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.=.1.3.3.1.3.5.0.3.9.7.0.5.1.0.8.3.6.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.5.9.1.e.c.a.b.-.e.6.1.9.-.4.e.a.b.-.a.b.a.c.-.c.d.6.7.4.5.d.3.9.6.7.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.7.8.0.9.e.e.6.-.f.3.d.e.-.4.a.d.b.-.9.f.1.b.-.1.0.b.0.f.e.e.8.d.1.5.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.k.O.i.a.W.L.N.K.X.p.j.a.y.W.e.M...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.7.f.0.-.0.0.0.1.-.0.0.1.f.-.c.b.0.8.-.9.5.f.9.9.c.f.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Nov 21 11:32:49 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	68898
Entropy (8bit):	2.2593657814055566
Encrypted:	false
SSDEEP:	384:CO95B3xDKkgXzqqCuQ922tpxKs1Tmg32J2TZO:/5Fx7RqCUqFrNO
MD5:	6FDB4190A9D1E0E7993BEF4AC6CF4903
SHA1:	709D61049D6C6D2E333A046DC248625624F7AF3B
SHA-256:	78FB31A09D0A60E4A2684787E690065C7663FC5172BE2078F42074678A6B3CA7
SHA-512:	A28808A8FEFED34B2536C210B9315D3FBEEECF7D29D900F0D08683578ED3939CFF4061546723003191FDEBDEB393840AFDB813BA5FEB5AC6282DA040F9CE227
Malicious:	false

Preview:	MDMP..... .....a{c.....H.....d@.....`.....8.....T.....H.....\&.....H(.....U.....B.....(... ...Lw.....3.z...T.....a{c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Nov 21 11:32:50 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	67910
Entropy (8bit):	2.2872930224451897
Encrypted:	false
SSDEEP:	192:Usoh09UmSpt3w2JcK/MgXY4aOC5eJraHi7NbVpEtxmtROgM43SbNYzoL:UN09qt3wDKkgXzlCcSe5pEtxmmg3eY4
MD5:	E2BEE3284D5782BF1CD920884AA0DDC0
SHA1:	3ABFC6B18012763101755546F05106E4DCF0B051A
SHA-256:	3435E6312400AD0F6341025145BA005652C7F38DE3F1833F0584D4378F3258CB
SHA-512:	5D99ED0613DF6F616F8554C4C597BF842265C3545BF5E4DA86923D87F56D4B757B3F4695167D81E4AA5B7A28AD677F8AA6CA02489BD780DD253094D8E1B8AA4
Malicious:	false
Preview:	MDMP..... .....a{c.....H.....d@.....`.....8.....T.....N.....\&.....H(.....U.....B.....(... ...Lw.....VK...T.....x....a{c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8722
Entropy (8bit):	3.6995272588026613
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi40jva6YNeEgmfZlfSmjqCprs89bPzqkfDFm:RrlsNizjva6Y0EgmfZlfS6rPzRfs
MD5:	BE46A1CF0D47BF92350C02FBB7BC6DCE
SHA1:	752B0D5513D543E34D6156EE78ECB3AA2CB7F583
SHA-256:	2847471816764542AAD97F3B098092F28B49B4CFC309CD1A7B52518DAF3CFECE
SHA-512:	C943406F61C34B3189F52B465875FC5C13458D5425419D958E54A4EC4F5483906581DDC7EB75CE3B39671AA0B147B2C8036212AED5FE4ABB5EA7448E00C1284E
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.>.6.1.2. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4751
Entropy (8bit):	4.494164486999496
Encrypted:	false
SSDEEP:	48:cvIwSD8zsblJgtBI91pWgc8sqYjrD/8fm8M4JCyCF2FW2yq85m2WZESC5Sgd:uITfb/LYgrsqYDkJK2LVvgd
MD5:	1AD542F6150D682107751BA46FFBB1CF
SHA1:	44F9DB01B37E1BAE1E3B8A74C67D2549D16E51A3
SHA-256:	147687BCE9BB3A5FE3746E68606ED2BBE919299D7D41FB7CEBADD846F879A66C
SHA-512:	376FEDF4CE7DB621ABA2739870C450521EC08DF77F28AD3935F9DB6719114226A9E0346C2CB3B1D9D294AF39CA8F192C4174076354635F41D851B066936E05CF
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="1789723" />.. <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\WER2452.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8520
Entropy (8bit):	3.695214149866878
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi9VIB5BR6YtdqMgmfZlfSmjqCprS89bPjffJwFm:RrlsNiPl/H6YXqMgmfZlfS65P7fh
MD5:	E5D5B3EE48668176FF7610C85F71B56F
SHA1:	B901413E9C393AA46786DC36773BA7031D16921A
SHA-256:	0989754C096D226569827F2C2BFBC6403C77B962534771CC1868E29BBA1B3631
SHA-512:	B386D181783FD965E11F7920958E9BFC0B33B3B62D390E8EE2D04E239BA67ED78F8BB799BD30FF4A2AC033053F46BC78BC5E7C09A012BEDC0A5DF096D5BBBE85
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.>.2.4.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4751
Entropy (8bit):	4.493494717828344
Encrypted:	false
SSDEEP:	48:cvIwSD8zsblJgtBl91pWgc8sqYjr0F8fm8M4JCyCF2Fsyq85m23ZESC5S2d:uITfb/LYgrsqYPJAKVv2d
MD5:	0D9B86BE737702FE9B1E0C59F154EA73
SHA1:	D5FCD44963ADAC173C1B34308CF6F2C5EF1ADBCC
SHA-256:	388A076160B1FD20113D856E8A9B2F9DFC64034E371B4FE06831AD9A63672DA5
SHA-512:	95DD60EBECD29740A969C0FBE95E2CDFE90DAE51398DA0F303206B95D9CED8E56D6274D931BB3CA5FA531ED59BBFF85FF51C5B2E34E18CD95BFB25EC828A7C33
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="1789723" />.. <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" />..

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.7768867083811415
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	kOiaWLNKXpjayWeM.dll
File size:	908800
MD5:	b7d93d2b47d14264b8b986b2d8fc7a49
SHA1:	9310b16c2d7f9195c65cdbecf8c5648525cb80e5
SHA256:	139c1faa496ae6c7d7c5140b9f4ac4e34f153bf40cd080c856b96bbd7ae716d2
SHA512:	ed83e77a65b7487c89bab393ecff7ea4315a319361e024196664903fd7ef2d42570d606d38a1554365c448d26b18c1b553bef78b708a2c9abfdf72036c599f5b
SSDEEP:	12288:A0BQgtzAxM8q6BkmkxisTsxwJzCQ6TZ56lu4Vp4y1F9SFXCwQwbk:Ar6zAxVq6Bkm7saIzCXTZxUJFcJ
TLSH:	4315BF12B3E503B9F4B7E139CA6A4A51EBB2BC4B5630E30F03E491966F23751493E716
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3.....=...Q.....Q.....Q.>.....Q.....Rich.....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180015150
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, NX_COMPAT
Time Stamp:	0x6364FEB9 [Fri Nov 4 11:59:53 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	c8d1998b80cffee902d21a3223b8978f

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007F9D64CFE257h
call 00007F9D64CFE340h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F9D64CFE0C0h
int3
int3

Copyright Joe Security LLC 2022

Instruction
int3
dec eax
and dword ptr [ecx+10h], 00000000h
dec eax
lea eax, dword ptr [000692FCh]
dec eax
mov dword ptr [ecx], eax
dec eax
mov eax, ecx
dec eax
mov dword ptr [ecx+08h], edx
ret
int3
dec eax
sub esp, 48h
dec eax
lea ecx, dword ptr [esp+20h]
call 00007F9D64CFCF83h
dec eax
lea edx, dword ptr [000C0483h]
dec eax
lea ecx, dword ptr [esp+20h]
call 00007F9D64CFF7FAh
int3
dec eax
sub esp, 48h
dec eax
lea ecx, dword ptr [esp+20h]
call 00007F9D64CEA43Bh
dec eax
lea edx, dword ptr [000C0383h]
dec eax
lea ecx, dword ptr [esp+20h]
call 00007F9D64CFF7DAh
int3
jmp 00007F9D64D3CDC0h
int3
int3
int3
inc eax
push ebp
dec eax
mov ebp, esp
dec eax
sub esp, 20h
dec eax
and dword ptr [ebp+18h], 00000000h
dec eax
lea ecx, dword ptr [ebp+18h]
call dword ptr [00067FC8h]
dec eax
mov eax, dword ptr [ebp+18h]
dec eax
mov dword ptr [ebp+10h], eax
call dword ptr [0006815Ah]
mov eax, eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xd59a0	0x6c0	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd6060	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe2000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0xdb000	0x5808	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe3000	0x914	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xcc8d0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xcc8f0	0x138	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7d000	0x5b0	.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	0x7b730	0x7b800	False	0.4151379048582996	zlib compressed data	6.500974730197073	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7d000	0x5a436	0x5a600	False	0.5386329745850622	data	6.216561858499759	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd8000	0x2dd8	0x1400	False	0.16875	data	2.74154034211106	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0xdb000	0x5808	0x5a00	False	0.5075086805555555	data	5.885478337065417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0xe1000	0xf4	0x200	False	0.3125	data	2.4589036841990084	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xe2000	0x1e0	0x200	False	0.52734375	data	4.711413092530877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe3000	0x914	0xa00	False	0.500390625	data	5.232229159197526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xe2060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
gdiplus.dll	GdipDrawString, GdipFree, GdiplusStartup, GdipAlloc, GdipDeleteFont, GdipCreateFont, GdipDeleteFontFamily, GdipCreateFontFamilyFromName, GdipGetVisibleClipBoundsI, GdipDrawImageI, GdipFillRectangleI, GdipDrawLineI, GdipDeleteGraphics, GdipCreateFromHDC, GdipCreateBitmapFromScan0, GdipGetImageGraphicsContext, GdipDisposeImage, GdipCloneImage, GdipDeletePen, GdipCreatePen1, GdipCreateLineBrushFromRectI, GdipCreateSolidFill, GdipDeleteBrush, GdipCloneBrush
CRYPT32.dll	CryptStringToBinaryA

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, WideCharToMultiByte, MultiByteToWideChar, GetCommandLineA, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindFirstFileExW, GetConsoleOutputCP, WriteFile, ReadConsoleW, GetProcessHeap, SetConsoleCtrlHandler, GetCommandLineW, CloseHandle, GetLastError, GetCurrentProcessId, CreateThread, GetVersionExA, VirtualAlloc, CreateToolhelp32Snapshot, Process32First, Process32Next, DeviceIoControl, ReleaseMutex, WaitForSingleObject, CreateMutexA, SetThreadExecutionState, CreateFileW, FindClose, FindFirstFileW, FindNextFileW, FlushFileBuffers, GetDiskFreeSpaceExW, GetStringTypeW, SetFilePointerEx, GetFileInformationByHandle, GetLogicalDriveStringsW, GetVolumeInformationW, GetVolumePathNameW, GetVolumeNameForVolumeMountPointW, Sleep, GetCurrentProcess, GetSystemTime, GetSystemTimeAsFileTime, FormatMessageW, SystemTimeToFileTime, FindFirstVolumeMountPointW, FindNextVolumeMountPointW, FindVolumeMountPointClose, GetLongPathNameW, GetShortPathNameW, GetModuleFileNameW, LocalFileTimeToFileTime, ReadFile, DosDateTimeToFileTime, GetConsoleMode, HeapReAlloc, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, GetLocaleInfoW, LCMapStringW, CompareStringW, GetTimeFormatW, GetDateFormatW, FlsFree, FlsSetValue, FlsGetValue, FlsAlloc, GetTempPathW, GetFileType, GetStdHandle, HeapFree, HeapAlloc, GetDriveTypeW, GetFileSizeEx, RtlUnwind, SetStdHandle, HeapSize, SetEndOfFile, WriteConsoleW, OutputDebugStringW, GetFileAttributesExW, GetCurrentThread, DeleteFileW, GetTimeZoneInformation, GetModuleHandleExW, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentThreadId, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, RtlPcToFileHeader, RaiseException, RtlUnwindEx, InterlockedPushEntrySList, InterlockedFlushSList, SetLastError, EncodePointer, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, ExitProcess
USER32.dll	ShowWindow, LoadStringA, LoadIconA, LoadCursorA, MessageBoxW, InvalidateRect, EndPaint, BeginPaint, UpdateWindow, SetTimer, CreateWindowExW, RegisterClassExA, PostQuitMessage, DefWindowProcA, DispatchMessageA, TranslateMessage, GetMessageA
GDI32.dll	GetStockObject
ADVAPI32.dll	RegQueryValueExW, RegCreateKeyExW, RegCloseKey, LookupPrivilegeValueA, AdjustTokenPrivileges, OpenProcessToken
SHELL32.dll	CommandLineToArgvW
ole32.dll	CoLoadLibrary

Exports

Name	Ordinal	Address
?AddArrayString@JKDefragLib@@QEAAPEAPEA_WPEAPEA_WPEA_W@Z	1	0x180005f7c
?CallShowStatus@JKDefragLib@@QEAAXPEAUDefragDataStruct@@HH@Z	2	0x180006a7c
?ColorizeItem@JKDefragLib@@QEAAXPEAUDefragDataStruct@@PEAUItemStruct@@_K2H@Z	3	0x180006f30
?DeleteItemTree@JKDefragLib@@QEAAXPEAUItemStruct@@@Z	4	0x18000adc0
?FragmentCount@JKDefragLib@@QEAAHPEAUItemStruct@@@Z	5	0x18000bcd0
?GetItemLcn@JKDefragLib@@QEAA_KPEAUItemStruct@@@Z	6	0x18000c048
?GetLongPath@JKDefragLib@@QEAAPEA_WPEAUDefragDataStruct@@PEAUItemStruct@@@Z	7	0x18000c06c
?GetShortPath@JKDefragLib@@QEAAPEA_WPEAUDefragDataStruct@@PEAUItemStruct@@@Z	8	0x18000c124
?IsFragmented@JKDefragLib@@QEAAHPEAUItemStruct@@_K1@Z	9	0x18000c1dc
?MatchMask@JKDefragLib@@QEAAHPEA_W0@Z	10	0x18000c290
?RunJkDefrag@JKDefragLib@@QEAAXPEA_WHHNPEAPEA_W1PEAH1@Z	11	0x18000dca0
?ShowHex@JKDefragLib@@QEAAXPEAUDefragDataStruct@@PEAE_K@Z	12	0x18000ecb4
?SlowDown@JKDefragLib@@QEAAXPEAUDefragDataStruct@@@Z	13	0x18000ee6c
?StopJkDefrag@JKDefragLib@@QEAAXPEAHH@Z	14	0x18000ef50
?SystemErrorStr@JKDefragLib@@QEAAXKPEA_W_K@Z	15	0x18000efac
?TreeBiggest@JKDefragLib@@QEAAPEAUItemStruct@@PEAU2@@Z	16	0x18000f07c
?TreeDetach@JKDefragLib@@QEAAXPEAUDefragDataStruct@@PEAUItemStruct@@@Z	17	0x18000f09c
?TreeFirst@JKDefragLib@@QEAAPEAUItemStruct@@PEAU2@H@Z	18	0x18000f1cc
?TreeInsert@JKDefragLib@@QEAAXPEAUDefragDataStruct@@PEAUItemStruct@@@Z	19	0x18000f208
?TreeNext@JKDefragLib@@QEAAPEAUItemStruct@@PEAU2@@Z	20	0x18000f3bc
?TreeNextPrev@JKDefragLib@@QEAAPEAUItemStruct@@PEAU2@H@Z	21	0x18000f3f8
?TreePrev@JKDefragLib@@QEAAPEAUItemStruct@@PEAU2@@Z	22	0x18000f408
?TreeSmallest@JKDefragLib@@QEAAPEAUItemStruct@@PEAU2@@Z	23	0x18000f444
?stristr@JKDefragLib@@QEAAPEADPEAD0@Z	24	0x18000f964
?stristrW@JKDefragLib@@QEAAPEA_WPEA_W0@Z	25	0x18000f9c4
DllRegisterServer	26	0x180003218

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
192.168.2.3218.38.121.17497144432404324 11/21/22-03:33:25.830611	TCP	2404324	ET CNC Feodo Tracker Reported CnC Server TCP group 13	49714	443	192.168.2.3	218.38.121.17

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2022 03:33:25.830610991 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:25.830670118 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:25.830774069 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:25.834296942 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:25.834327936 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:26.678919077 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:26.679049015 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:26.684890032 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:26.684900045 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:26.685220003 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:26.734738111 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:26.972662926 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:26.972714901 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:28.495560884 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:28.495716095 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:28.495820045 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:28.497793913 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:28.497824907 CET	443	49714	218.38.121.17	192.168.2.3
Nov 21, 2022 03:33:28.497879982 CET	49714	443	192.168.2.3	218.38.121.17
Nov 21, 2022 03:33:28.497911930 CET	443	49714	218.38.121.17	192.168.2.3

HTTP Request Dependency Graph

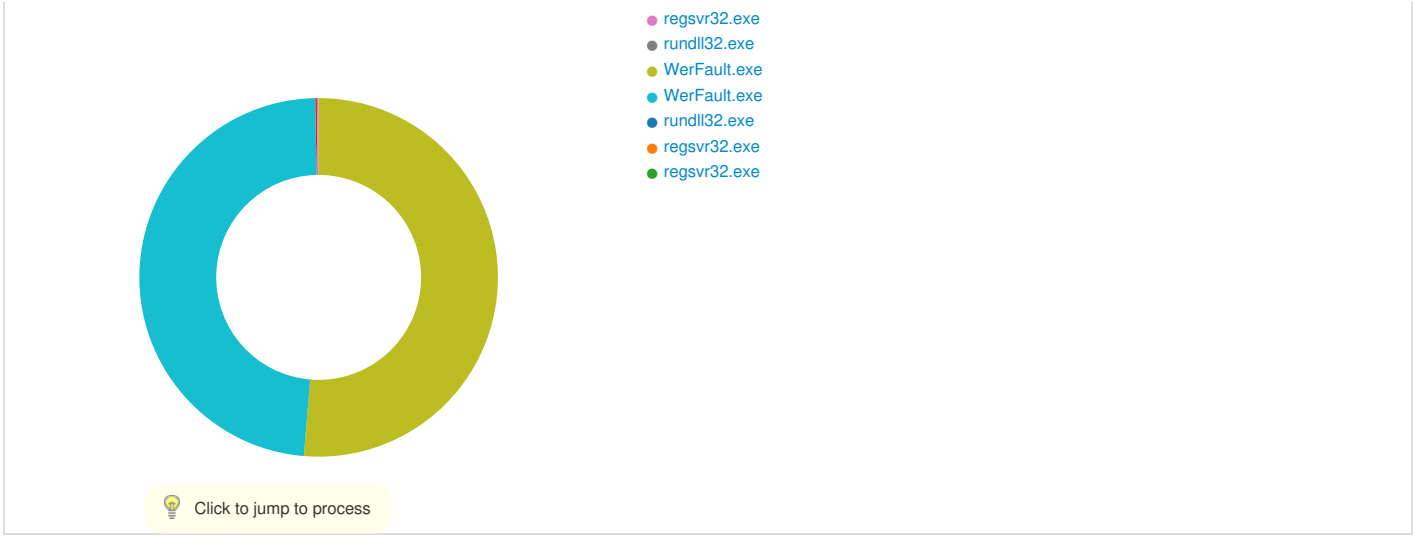
- 218.38.121.17

Statistics

Behavior

- loaddll64.exe
- conhost.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe

Copyright Joe Security LLC 2022



System Behavior

Analysis Process: loaddll64.exe PID: 6112, Parent PID: 3452

General

Target ID:	0
Start time:	03:32:44
Start date:	21/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll"
Imagebase:	0x7ff600720000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6096, Parent PID: 6112

General

Target ID:	1
Start time:	03:32:44
Start date:	21/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Reputation:	high

Analysis Process: cmd.exe PID: **6044**, Parent PID: **6112**

General

Target ID:	2
Start time:	03:32:45
Start date:	21/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll",#1
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6076**, Parent PID: **6112**

General

Target ID:	3
Start time:	03:32:45
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll
Imagebase:	0x7ff7f5e80000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.254435708.0000000002401000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.254242832.000000000B00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\WVVZhuligM\KuLiEStgIluewHbC.dll:Zone.Identifier	success or wait	1	241874C	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6128**, Parent PID: **6044**

General	
Target ID:	4
Start time:	03:32:45
Start date:	21/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll",#1
Imagebase:	0x7ff63eb10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.253014513.0000022AB0991000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.287369701.0000022AB0780000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.254193655.0000022AB0991000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.253580195.0000022AB0780000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.287814441.0000022AB0991000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.251796872.0000022AB0780000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2424**, Parent PID: **6112**

General	
Target ID:	5
Start time:	03:32:45
Start date:	21/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll,?AddArrayString@JKDefragLib@@QEAAPEAPEA_WPEAPEA_WPEA_W@Z
Imagebase:	0x7ff63eb10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.253546936.0000021CE85C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.255111695.0000021CE8590000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.287467703.0000021CE8590000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.255327053.0000021CE85C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.253497739.0000021CE8590000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.287612874.0000021CE85C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **5252**, Parent PID: **6076**

General	
Target ID:	8
Start time:	03:32:48
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\WVVZhuligM\KuLiEStglluewHbC.dll"
Imagebase:	0x7ff7f5e80000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.768911804.00000000029C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000008.00000002.767607073.0000000000F14000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.768771937.0000000002990000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	KuLiEStglluewHbC.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\WVVZhuligM\KuLiEStglluewHbC.dll"	success or wait	1	29E69BB	RegSetValueExW

Analysis Process: rundll32.exe PID: **5228**, Parent PID: **6112**

General

Target ID:	9
Start time:	03:32:48
Start date:	21/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll,?CallShowStatus@JKDefragLib@@QEAAXPEAUDefragDataStruct@@HH@Z
Imagebase:	0x7ff63eb10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **5204**, Parent PID: **6128**

General

Target ID:	10
Start time:	03:32:48
Start date:	21/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6128 -s 480
Imagebase:	0x7ff679980000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC119E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD57D.tmp.csv	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD58E.tmp.txt	success or wait	1	7FFC119DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 61 7b 63 fd 05 12 00 00 00 00 00	MDMP a{c	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	10464	6	00 00 00 00 00 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 28 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 33 fd 7a 02 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 fd 61 7b 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 30 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 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UB(Lw3zTa{c0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	11556	1232	fd 0b 3d fd 2a 02 00 00 00 00 00 00 00 00 00 00 00 7b fd 2a 02 00 00 fd 00 00 00 00 00 00 00 fd 03 00 00 00 00 00 00 01 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	17752	8	4f 7e 12 32 fd 7f 00 00	O~2	success or wait	78	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	61802	256	48 fd fd 24 00 01 00 00 48 fd fd 24 fd 01 00 00 33 fd 4c fd fd 24 fd 01 00 00 4d fd fd 49 fd fd 44 fd fd 48 fd fd 44 0f fd fd 44 fd fd 4d fd fd 0f fd fd fd 09 00 fd 79 10 fd fd fd fd 0f fd fd 00 00 00 48 fd fd 0f fd fd fd 09 00 4d fd fd 0f fd fd fd 09 00 fd 41 74 44 0b fd 0f fd fd 18 0f fd fd fd 09 00 fd 41 78 01 0f fd fd fd 09 00 40 fd fd 0f 0f fd 17 09 00 49 fd 78 fd 0f 0d 0f fd 7f 0f 05 0f fd fd fd 09 00 fd 47 0f 3f 0f fd fd fd 09 00 48 fd fd 0f fd 4b 01 00 00 fd 7d fd 05 0f fd 17 09 00 41 fd fd 4d fd c3 fd 02 4c fd fd 48 fd fd fd 37 01 00 00 48 fd fd fd 05 fd 00 15 00 fd 01 0f fd 4d fd 09 00 48 fd fd 0f fd fd 00 00 00 48 fd fd 45 fd fd 0f fd fd fd 09 00 48 fd fd 48 fd fd 24 00 01 00 00 48 33 fd fd fd 07 00 48 fd fd 18 01 00 00 41 5f 41 5e	HH3L$MIDHDDMyHMAtDAx@IxG?HK}AMLH7HMHHEHH$H3HA_A^	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	12788	1232	10 00 00 00 00 00 00 00 20 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 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	5852	3960	00 00 fd 2c fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 2d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 fd fd 2a 02 00 00 14 fd fd fd 2a 02 00 00 00 00 fd fd 2a 02 00 00 33 01 00 00 04 00 00 00 fd fd 1b 32 fd 7f 00 00 fd fd 1b 32 fd 7f 00 00 00 fd 2a 02 00 00 fd 58 fd fd fd fd fd 01 00 10 fd fd 2a 02 00 00 14 fd fd fd 2a 02 00 00 00 00 fd fd 2a 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	62058	6840	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6F.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0f 00 00 fd 07 00 00 0d 00 00 00 14 0f 00 00 48 17 00 00 05 00 00 00 fd 04 00 00 64 40 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 48 13 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 5c 26 00 00 16 00 00 00 fd 00 00 00 48 28 00 00	Hd@`8TH\&H(	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6128</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4912</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1228	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1314	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1374	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1428	96	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 32 00 32 00 30 00 33 00 34 00 34 00 32 00 34 00 32 00 31 00 37 00 36 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>2203442421760</PeakVirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1534	80	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 32 00 32 00 30 00 33 00 34 00 34 00 32 00 34 00 31 00 33 00 35 00 36 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>2203442413568</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1624	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 33 00 36 00 31 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3615</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1698	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1702	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1708	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 30 00 30 00 32 00 34 00 33 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>10002432</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1806	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1810	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1816	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 30 00 30 00 32 00 34 00 33 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>10002432</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1898	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1902	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	1908	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 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 50 00 61 00 67 00 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>173464</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2022	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2026	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2032	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 32 00 36 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>173264</QuotaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2130	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2134	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2140	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 33 00 31 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 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>31320</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2264	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2268	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2274	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 33 00 30 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>30968</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2382	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2386	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2392	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 32 00 39 00 39 00 34 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2994176</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2478	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 32 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3002368</PeakPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2570	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2574	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2580	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 32 00 39 00 39 00 34 00 31 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2994176</PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2652	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2656	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2660	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2706	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2710	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2714	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2744	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2748	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2754	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2794	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2798	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2806	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6044</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2836	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2840	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2848	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2908	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2912	2	09 00		success or wait	4	7FFC119DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	2920	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3010	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3014	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3022	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 30 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5081</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3076	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3288	96	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 32 00 32 00 30 00 33 00 33 00 37 00 30 00 33 00 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22033 70369024 </PeakVirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3384	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3388	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3398	80	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 32 00 32 00 30 00 33 00 33 00 37 00 30 00 33 00 36 00 39 00 30 00 32 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>220337036 9024</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3492	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>788</ PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3578	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 31 00 32 00 32 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2 912256</P eakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3688	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 31 00 32 00 32 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>29122 56</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3782	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	3908	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 00 36 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>27664</QuotaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4018	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 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>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4154	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 30 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>3800</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4274	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 35 00 33 00 39 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3153920</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4350	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4354	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4364	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 35 00 33 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3153920</PeakPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4456	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4460	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4470	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 35 00 33 00 39 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3153920</PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4554	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4604	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4610	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4660	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4698	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4746	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4792	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	8	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	16	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	4862	116	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 6b 00 4f 00 69 00 61 00 57 00 4c 00 4e 00 4b 00 58 00 70 00 6a 00 61 00 79 00 57 00 65 00 4d 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe_kOiaWLNKXpjayWeM.dll</Parameter0>	success or wait	8	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5530	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5534	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5536	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5582	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	12	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	5628	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6182	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6186	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6188	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6234	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6280	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6374	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6378	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6382	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 75 00 68 00 71 00 64 00 6f 00 61 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>uhqdoa, Inc.</SystemManufacturer>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6488	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6492	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6496	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 75 00 68 00 71 00 64 00 6f 00 61 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>uhqdoa7,1</SystemProductName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6592	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6596	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6600	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6720	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6724	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6728	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 37 00 39 00 36 00 31 00 33 00 30 00 36 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>1607961306</OSInstallDate>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6810	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6814	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6818	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6920	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6924	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6928	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7002	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7048	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7090	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7186	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7190	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7192	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7228	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7232	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7234	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	6	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7266	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7512	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7516	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7518	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7544	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7548	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7550	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 31 00 54 00 31 00 31 00 3a 00 33 00 32 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-21T11:32:50Z">	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7650	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7654	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7658	262	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 32 00 38 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 32 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 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 31 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	<Process AsId="289" PID="6128" UptimeMS="1687" TimeSinceCreationMS="1687" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7920	4	0d 00 0a 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7924	2	09 00		success or wait	6	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	7930	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 39 00 32 00 32 00 38 00 31 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5922816" TimelineUnitShift="12" Timeline="1"/>	success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8312	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8332	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8336	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8338	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8376	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8380	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8382	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8420	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8424	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8428	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 35 00 39 00 31 00 65 00 63 00 61 00 62 00 2d 00 65 00 36 00 31 00 39 00 2d 00 34 00 65 00 61 00 62 00 2d 00 61 00 62 00 61 00 63 00 2d 00 63 00 64 00 36 00 37 00 34 00 35 00 64 00 33 00 39 00 36 00 37 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f591ecab-e619-4eab-abac-cd6745d3967f</Guid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8526	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8530	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8534	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 31 00 54 00 31 00 31 00 3a 00 33 00 32 00 3a 00 35 00 30 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>2022-11-21T11:32:50Z</CreationTime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8632	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8636	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8638	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8678	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER222F.tmp.WERInternalMetadata.xml	8682	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER232A.tmp.xml	0	4751	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813\Report.wer	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813\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	162	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_14085813\Report.wer	10866	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 33 00 36 00 36 00 37 00 37 00 32 00 32 00 35 00	MetadataHash=-1536677225	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC119DE3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFC11A01D2D	unknown

Copyright Joe Security LLC 2022

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFC11A01D2D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E AF DE FC 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00

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	7FFC119E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD715.tmp.csv	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD726.tmp.txt	success or wait	1	7FFC119DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 61 7b 63 fd 05 12 00 00 00 00 00	MDMP a{c	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	10464	6	00 00 00 00 00 00		success or wait	1	7FFC119DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 28 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 56 4b fd 01 00 00 54 05 00 00 fd 03 00 00 78 09 00 00 fd 61 7b 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 30 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 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UB(LwVKTxa{c0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	11556	1232	01 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 fd fd 1c 02 00 00 01 00 00 00 00 00 00 00 fd 0b 70 fd 1c 02 00 00 7f 00 00 00 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	17752	2040	76 fd 06 32 fd 7f 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 10 00 00 00 00 00 00 00 48 fd fd fd 37 00 00 00 41 fd fd fd 37 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 fd 72 fd 37 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 40 43 fd fd 1c 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 38 30 fd fd 1c 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	12788	1232	fd fd fd fd fd fd fd 20 00 00 00 00 00 00 fd fd fd fd fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	9820	644	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 fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 06 36 01 00 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 fd 69 03 00 00 00 00 00 fd 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 35 34 1b 00 00 00 00 00 0b fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 0b fd 04 00 00 00 00 00 7a fd fd 5c 00 00 00 00 19 fd fd 15 00 00 00 00 33 7f fd 0f 00 00 00 00 2a fd 68 01 00 00 00 00 3d fd 00 00 fd fd 00 00 fd fd 05 00 2c fd 0a 00 0b fd 04 00 06 fd 1f 00 0b fd 04 00 fd 58 1f 00 fd 19 01 00 fd 60 0e 00 00 00 00 00 fd 08 11 00 14 38 04 00 51 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 02 00	Zb6ip54@z\3*h=,X`8QU	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	61178	6732	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2173.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0f 00 00 fd 07 00 00 0d 00 00 00 14 0f 00 00 48 17 00 00 05 00 00 00 fd 04 00 00 64 40 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 12 00 00 4e fd 00 00 15 00 00 00 fd 01 00 00 5c 26 00 00 16 00 00 00 fd 00 00 00 48 28 00 00	Hd@`8TN\&H(	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2424</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000000</CmdLineSignature>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 39 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5398</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1228	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1314	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1374	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1428	96	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 32 00 32 00 30 00 33 00 34 00 34 00 32 00 34 00 32 00 31 00 37 00 36 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>2203442421760</PeakVirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1534	80	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 32 00 32 00 30 00 33 00 34 00 34 00 32 00 34 00 31 00 33 00 35 00 36 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>2203442413568</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1624	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 33 00 36 00 32 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3627</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1698	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1702	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1708	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 30 00 33 00 31 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10031104</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1806	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1810	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1816	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 30 00 33 00 31 00 31 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10031104</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1898	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1902	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	1908	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 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 50 00 61 00 67 00 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>173464</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2022	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2026	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2032	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 33 00 32 00 36 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>173264</QuotaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2130	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2134	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2140	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 33 00 31 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>31512</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2264	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2268	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2274	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 33 00 31 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>31160</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2382	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2386	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2392	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 31 00 34 00 36 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>3014656</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2478	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 32 00 32 00 38 00 34 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>30 22848</Pe akPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2570	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2574	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2580	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 31 00 34 00 36 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>3014656 </PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2652	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2656	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2660	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2706	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2710	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2714	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2744	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2748	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2754	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2794	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2798	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2806	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6112</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2836	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2840	2	09 00		success or wait	4	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2848	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 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>loaddll64.exe</ImageName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2920	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2924	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	2932	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3022	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3026	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3034	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 38 00 34 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5846</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3088	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3178	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3242	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3300	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 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4345114624</PeakVirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3404	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 33 00 34 00 31 00 31 00 34 00 39 00 36 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4341149696</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3492	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 34 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>649</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3578	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 33 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2334720</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3688	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 32 00 32 00 34 00 33 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>23224 32</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3782	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolU sage>73744 </QuotaPeakPagedPool Usage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	3908	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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 >65824</Qu otaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4018	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>40 72</QuotaPeakNonPage dPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4154	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 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>2984</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4274	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>483328</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4348	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4352	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4362	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 00 36 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>495616</PeakPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4452	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4456	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4466	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>483328</PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4536	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4540	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4548	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4594	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4598	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4604	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4646	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4650	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4654	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4686	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4690	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4692	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4734	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4738	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4740	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4778	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4782	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4786	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4848	4	0d 00 0a 00		success or wait	8	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4852	2	09 00		success or wait	16	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	4856	116	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 6b 00 4f 00 69 00 61 00 57 00 4c 00 4e 00 4b 00 58 00 70 00 6a 00 61 00 79 00 57 00 65 00 4d 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe_kOiaWLNKXpjayWeM.dll</Parameter0>	success or wait	8	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5524	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5528	2	09 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5530	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5576	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	12	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	5622	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6176	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6180	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6182	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6228	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6274	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6368	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6372	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6376	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 75 00 68 00 71 00 64 00 6f 00 61 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>uhqdoa, Inc.</SystemManufacturer>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6482	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6486	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6490	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 75 00 68 00 71 00 64 00 6f 00 61 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>uhqdoa7,1</SystemProductName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6586	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6590	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6594	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6722	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 37 00 39 00 36 00 31 00 33 00 30 00 36 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>1607961306</OSInstallDate>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6804	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6808	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6812	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6914	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6918	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6922	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	6996	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7042	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7084	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7186	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	7FFC119DE9F7	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7222	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7226	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7228	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7260	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7506	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7510	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7512	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7538	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7542	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7544	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 31 00 54 00 31 00 31 00 3a 00 33 00 32 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-21T11:32:50Z">	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7644	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7648	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7652	262	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 32 00 39 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 34 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 31 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 31 00 38 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="290" PID="2424" UptimeMS="2187" TimeSinceCreationMS="2187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	7924	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 39 00 32 00 32 00 38 00 31 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5922816" TimelineUnitShift="12" Timeline="1"/>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8102	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8106	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8110	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8130	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8134	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8136	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8174	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8178	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8180	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8218	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8222	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8226	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 66 00 65 00 39 00 64 00 61 00 31 00 32 00 2d 00 35 00 61 00 66 00 35 00 2d 00 34 00 35 00 61 00 63 00 2d 00 61 00 35 00 34 00 64 00 2d 00 31 00 36 00 30 00 39 00 36 00 39 00 65 00 38 00 62 00 31 00 33 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>1fe9da12-5af5-45ac-a54d-160969e8b13f</Guid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8324	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8328	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8332	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 31 00 54 00 31 00 31 00 3a 00 33 00 32 00 3a 00 35 00 30 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>2022-11-21T11:32:50Z</CreationTime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8430	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8434	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8436	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8476	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2452.tmp.WERInternalMetadata.xml	8480	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24EF.tmp.xml	0	4751	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4\Report.wer	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4\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	162	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_kOi_a748228d1b9ab9a1bb94dae9e0fac923745_f2877757_0d5857e4\Report.wer	10866	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 32 00 30 00 33 00 35 00 31 00 36 00 38 00 30 00 39 00 36 00	MetadataHash=-2035168096	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{242152ea-91f6-9c12-fea7-ca7749e75c6a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC119DE3FE	unknown

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

Analysis Process: rundll32.exe PID: **1788**, Parent PID: **6112**

General

Target ID:	12
Start time:	03:32:51
Start date:	21/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\kOiaWLNKXpjayWeM.dll,?ColorizeItem@JKDefragLib@@QEAAXPEAUDefragDataStruct@@PEAUItemStruct@@_K2H@Z
Imagebase:	0x7ff63eb10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6128, Parent PID: 3452

General

Target ID:	22
Start time:	03:33:38
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\WVVZhuligM\KuLiEStglluewHbC.dll
Imagebase:	0x7ff7f5e80000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000016.00000002.371644938.0000000002A00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000016.00000002.371681565.0000000002A31000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 5288, Parent PID: 6128

General

Target ID:	23
Start time:	03:33:42
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\WrWLj\BwssvzQrG.dll"
Imagebase:	0x7ff7f5e80000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly