




**ID:** 345555
**Sample Name:**
2760000.netprovfw.bin
**Cookbook:** default.jbs
**Time:** 16:27:00
**Date:** 28/01/2021
**Version:** 31.0.0 Emerald

# Table of Contents


Table of Contents 2
Analysis Report 2760000.netprovfw.bin 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Memory Dumps 4
Unpacked PEs 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
E-Banking Fraud: 5
Stealing of Sensitive Information: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 10
General 10
File Icon 11
Static PE Info 11
General 11
Entrypoint Preview 11
Rich Headers 12
Data Directories 12
Sections 13
Resources 13
Network Behavior 13
UDP Packets 13
Code Manipulations 14
Statistics 14

Behavior 14
System Behavior 14
Analysis Process: 2760000.netprovfw.exe PID: 3636 Parent PID: 5668 14
General 14
Analysis Process: WerFault.exe PID: 4852 Parent PID: 3636 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 16
Registry Activities 37
Key Created 37
Key Value Created 37
Disassembly 38
Code Analysis 38

Copyright null 2021

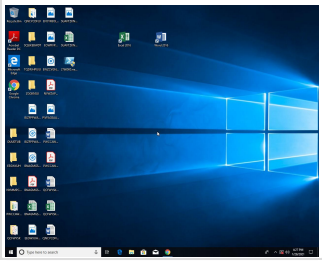
# Analysis Report 2760000.netprovfw.bin

## Overview

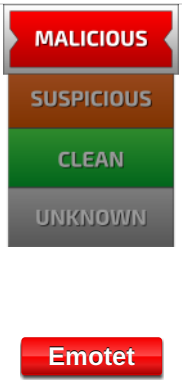
### General Information

| | |
|---|---|
| Sample Name: | 2760000.netprovfw.bin (renamed file extension from bin to exe) |
| Analysis ID: | 345555 |
| MD5: | 90478bb3273d74.. |
| SHA1: | 8fa8f069d4391a2.. |
| SHA256: | f865736f27acaac.. |

Most interesting Screenshot:



### Detection

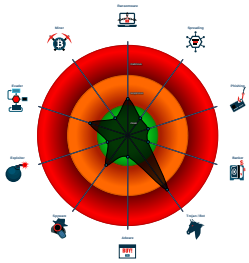



| | |
|---|---|
| Score: | 68 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- One or more processes crash
- PE file contains an invalid checksum
- PE file contains strange resources
- PE file does not import any functions

### Classification



## Startup

- **System is w10x64**
- 2760000.netprovfw.exe (PID: 3636 cmdline: 'C:\Users\user\Desktop\2760000.netprovfw.exe' MD5: 90478BB3273D74A7A4BAE530DEE87174)
  - WerFault.exe (PID: 4852 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3636 -s 640 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 2760000.netprovfw.exe | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.215311677.0000000002761000.00000020.00020000.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 00000000.00000000.206372217.0000000002761000.00000020.00020000.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |

### Unpacked PEs

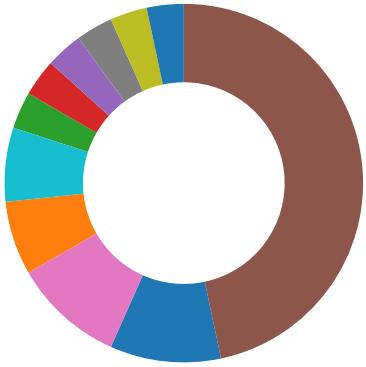
| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0.0.2760000.netprovfw.exe.2760000.0.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 0.2.2760000.netprovfw.exe.2760000.0.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |

Copyright null 2021

## Sigma Overview

No Sigma rule has matched

## Signature Overview



- AV Detection
- Compliance
- Spreading
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Stealing of Sensitive Information

Click to jump to signature section

### AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Compliance:



Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

### E-Banking Fraud:



Yara detected Emotet

### Stealing of Sensitive Information:



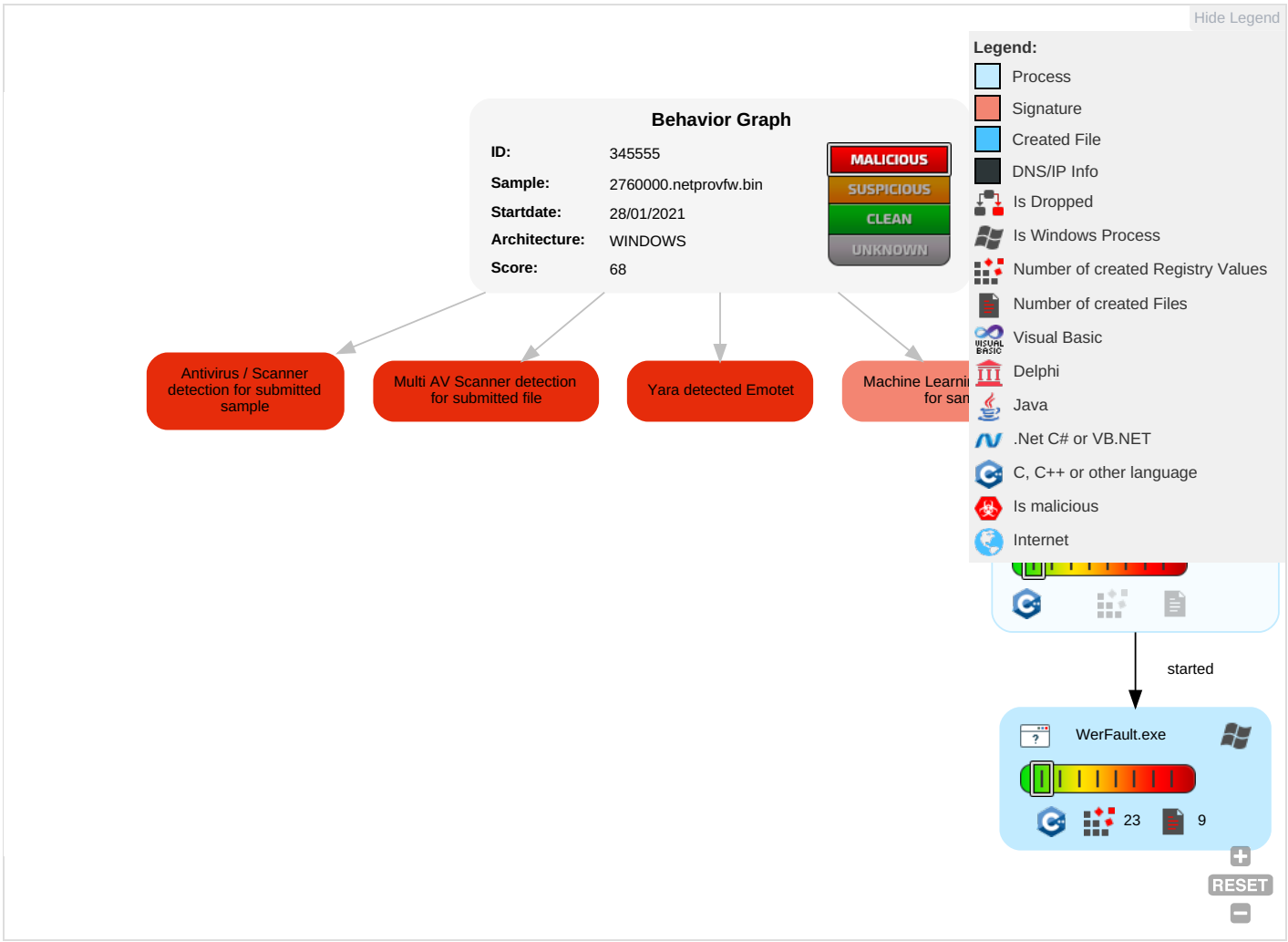
Yara detected Emotet

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Re Se Ef |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Virtualization/Sandbox Evasion 1 | Input Capture 1 | Security Software Discovery 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | Re Tr W Au |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Re Se Ef |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Software Packing 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Re W W Au |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 | Security Account Manager | File and Directory Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Ol De Cl Ba |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 2 | NTDS | System Information Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Software Packing | LSA Secrets | Remote System Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |

## 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 |
|---|---|---|---|---|
| 2760000.netprovfw.exe | 50% | Virustotal | | Browse |
| 2760000.netprovfw.exe | 79% | ReversingLabs | Win32.Trojan.Convagent | |
| 2760000.netprovfw.exe | 100% | Avira | TR/Crypt.XPACK.Gen | |
| 2760000.netprovfw.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.1.2760000.netprovfw.exe.2760000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.0.2760000.netprovfw.exe.2760000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |
| 0.2.2760000.netprovfw.exe.2760000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen | | Download File |

### Domains

No Antivirus matches

### URLs

**No Antivirus matches**

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Emerald |
| Analysis ID: | 345555 |
| Start date: | 28.01.2021 |
| Start time: | 16:27:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 2m 26s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 2760000.netprovfw.bin (renamed file extension from bin to exe) |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 3 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal68.troj.winEXE@2/4@0/0 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 100% (good quality ratio 99.3%)<br>• Quality average: 71.8%<br>• Quality standard deviation: 20.8% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Stop behavior analysis, all processes terminated |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): WerFault.exe<br>• Excluded IPs from analysis (whitelisted): 52.147.198.201, 52.255.188.83<br>• Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com |

Copyright null 2021

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 16:27:54 | API Interceptor | 1x Sleep call for process: WerFault.exe modified |

# Joe Sandbox View / Context

## IPs

No context

## Domains

No context

## ASN

No context

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

**C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_2760000.netprovf_50482980db6f70d047bdd5f2b763ef22b1cfde7_9c33c211_129efdf4\Report.wer**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 10994 |
| Entropy (8bit): | 3.7614659673061346 |
| Encrypted: | false |
| SSDEEP: | 96:zAaFnqcKJ1hskDRf2pXIQcQvc6QcEDMcw3Db+HbHg/uAnQ0DFV6Fq/TOiNkoJT4V:caF3VHBUZMXYjla/u7scS274ltkS+ |
| MD5: | 720CE52891513A7CE9B86362267F0DA5 |
| SHA1: | DEBB950A22077D504E7615EAF440772D1903A500 |
| SHA-256: | 694BB24B19E45591A31DD2B4F2744B883E902E1A59692CD4735E4DE3AC58CCC8 |
| SHA-512: | F211EAD3CFDE2F98CCB5ADBBCCD0D5C27D35201B0AE5BB4A70E0B5E23BAD30010BF26DA94F41497B1F938CD5F45D1400A2368A8E28D4FA08CF3C9C47317EF8CC |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.3.5.3.6.7.2.0.5.9.4.2.9.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.3.5.3.6.7.2.7.6.2.5.4.8.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.d.e.9.d.f.1.3.-.b.a.c.d.-.4.a.a.b.-.8.7.f.5.-.a.3.7.1.1.d.b.5.0.0.6.1.....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.=.a.1.1.3.7.b.7.7.-.b.d.f.0.-.4.d.d.7.-.8.b.3.6.-.6.2.2.3.0.1.0.9.7.5.0.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.2.7.6.0.0.0.0...n.e.t.p.r.o.v.f.w...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.e.3.4.-.0.0.0.1.-.0.0.1.7.-.e.c.3.9.-.3.2.9.3.d.5.f.5.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.0.f.c.c.3.2.5.5.9.8.9.5.0.a.9.b.b.8.c.a.5.b.6.5.8.9.1.d.6.8.6.0.0.0.0.f.f.f.f.!.0.0.0.0.8.f.a.8.f.0.6.9.d.4.3.9.1.a.2.1.3.4.6.d.e.6.5.a.5.e.e.7.2.9.a.d.6.e.f.5.6.a.6.0.!.2.7.6.0.0.0.0...n.e.t.p.r.o.v. |

**C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Fri Jan 29 00:27:52 2021, 0x1205a4 type |
| Category: | dropped |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | |
|---|---|
| Size (bytes): | 41726 |
| Entropy (8bit): | 2.2476995034013756 |
| Encrypted: | false |
| SSDEEP: | 192:A1X2ZQnnUJO7htz2SKwrdcMhMDyTROcb5Kszgeb:W/gSKaS1DyTRRblvb |
| MD5: | 87A7ABC2F6BEAB6144BC5B26B23AE74A |
| SHA1: | 90BC5F6AD1F9D5474FC3AB9F696FC6B37F65B421 |
| SHA-256: | A14D136A44ECE61B85B934F9A0F7CD91704847AEF659196F536710F0F5F478BB |
| SHA-512: | 6330C9B8B186F8FA0656C7FBF1AEF94BE11A519E6FE7D3511D7C7EF45D15B4288880564873F02F3B479541283DEC1F549255C73D6A4A90E60D6BDB38A4940C93 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MDMP..... .....V.`.....U.....B.....T.....GenuineIntelW.....T.....4....V.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ..... ..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... ..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8316 |
| Entropy (8bit): | 3.694070001122533 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNi526b6YS3SUnYsgmfJfGSwCprR889b+sWsfG4Km:RrlsNio6b6YiSUnYsgmfJ+SJp+s1fN7 |
| MD5: | D984D43F2B351442B894831AED8A541A |
| SHA1: | D17A0A15F90E05B8305E1593EB236CDE91B5CE5A |
| SHA-256: | 10AB7323E241217ECA9B43DAAC0C0AEDA00A17B42CEEEB9253DD45B505746688 |
| SHA-512: | 55FEB2D609DF9EBD3ECC5960280B666412F455E6E1565FBC01D03C2FC8F183DD1439C5402685C0C2CE95ED3CB6B6DF3ED448708A6AABB783C06899CA429F17E |
| Malicious: | false |
| Reputation: | low |
| 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.>.3.6.3.6.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81A.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4605 |
| Entropy (8bit): | 4.454386786497803 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zsxlJgtWI9EKWSC8Bq8fm8M4JzXYlFs8+q8I6ROC6vG6d:uITf53rSN9JR8JVvG6d |
| MD5: | 5EF659495C5F15CBFFB7E779342ECDF1 |
| SHA1: | 9E271CDB285588F5EE1A8F0D125EA0E6EB149E03 |
| SHA-256: | EC7E8E6E007E9BA87CF04894BD00BB64B1BAE5E8D8851B82B054BC0B12C08873 |
| SHA-512: | 9C386FE1DC6B6B8C5F7F62DAD5A39AF7AB911361F65CBD6880CA541B2FFEA2EE470E466251C44376F64946B00E5F7A3418CB6B69157006E59D3BF51B49EF8D9 |
| Malicious: | false |
| Reputation: | low |
| 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="837218" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

# Static File Info

## General

| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
|---|---|

## General

| | |
|---|---|
| Entropy (8bit): | 5.529033895906113 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | 2760000.netprovfw.exe |
| File size: | 350208 |
| MD5: | 90478bb3273d74a7a4bae530dee87174 |
| SHA1: | 8fa8f069d4391a21346de65a5ee729ad6ef56a60 |
| SHA256: | f865736f27acaaca93c530f82295fdddf9b97fc54f37732815e89ad660eb69e4 |
| SHA512: | 4df47075f24abd5882f27e22d39c6a73b1586ddd1757539387a885e3f112e1e00b4b97b4f68d91ef5662c7a3973ab350fe5e1e68d36943948ffa255315f51961 |
| SSDEEP: | 6144:Lt0Ju8YGNKXzJ7BapCK5d3klRzULOnWyjLsPhAQzqOY:x0J5nKXzJ4pdd3klnnWosPhnzqL |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.../.../.../...".J.....R.p.....R.K.....Rich/.....PE..L...M.._.....\.....v..... |

## File Icon



| | |
|---|---|
| Icon Hash: | c0d9f1f399a4c2c1 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x2765cd0 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x2760000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NO_ISOLATION, NX_COMPAT |
| Time Stamp: | 0x5F90A34D [Wed Oct 21 21:08:29 2020 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: | |

### Entrypoint Preview

| Instruction |
|---|
| call 00007F0628F9DD70h |
| mov eax, dword ptr [0276E2C4h] |
| test eax, eax |
| jne 00007F0628F9D50Dh |
| mov ecx, A2CE093Fh |
| call 00007F0628F9B77Dh |
| mov edx, B9B17DC0h |
| mov ecx, eax |
| call 00007F0628F9B6D1h |
| mov dword ptr [0276E2C4h], eax |
| push 00000000h |
| call eax |
| retn 0010h |
| push ecx |

| Instruction |
| --- |
| mov dword ptr [esp], 000021B4h |
| add dword ptr [esp], 00005AC3h |
| shl dword ptr [esp], 04h |
| mov eax, dword ptr [esp] |
| shl eax, 06h |
| mov dword ptr [esp], eax |
| or dword ptr [esp], CC87922Ah |
| xor dword ptr [esp], CDF7DF6Ah |
| mov eax, dword ptr [esp] |
| pop ecx |
| ret |
| int3 |
| push ecx |
| mov dword ptr [esp], 00002C7Ch |
| imul eax, dword ptr [esp], 2Dh |
| mov dword ptr [esp], eax |
| shl dword ptr [esp], 0Ch |
| xor dword ptr [esp], 9184714Ch |
| shl dword ptr [esp], 0Fh |
| or dword ptr [esp], 011C88C3h |
| xor dword ptr [esp], 59BE8863h |
| mov eax, dword ptr [esp] |
| pop ecx |
| ret |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |
| push ecx |
| mov dword ptr [esp], 00008067h |
| xor dword ptr [esp], 30B3246Ch |
| add dword ptr [esp], 000090BEh |
| xor dword ptr [esp], 30B43B69h |
| mov eax, dword ptr [esp] |
| pop ecx |
| ret |
| int3 |
| int3 |
| int3 |
| int3 |
| int3 |

## Rich Headers

| | |
| --- | --- |
| Programming Language: | • [ASM] VS2013 build 21005<br>• [LNK] VS2013 UPD4 build 31101 |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
| --- | --- | --- | --- |
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x10000 | 0x49800 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0xf000 | 0x74c | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x0 | 0x0 | |
| 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 | 0xb000 | 0xa600 | False | 0.544686558735 | data | 6.84651766717 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0xc000 | 0x1000 | 0x200 | False | 0.02734375 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xd000 | 0x2000 | 0xc00 | False | 0.851888020833 | data | 7.19591538106 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .reloc | 0xf000 | 0x1000 | 0x800 | False | 0.01123046875 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x10000 | 0x4a000 | 0x49800 | False | 0.348051525298 | data | 5.21306515691 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x102fc | 0x668 | data | | |
| RT_ICON | 0x10964 | 0x2e8 | dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2296940798, next used block 15239304 | | |
| RT_ICON | 0x10c4c | 0x1e8 | data | | |
| RT_ICON | 0x10e34 | 0x128 | GLS_BINARY_LSB_FIRST | | |
| RT_ICON | 0x10f5c | 0xea8 | data | | |
| RT_ICON | 0x11e04 | 0x8a8 | dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 14019316, next used block 14479096 | | |
| RT_ICON | 0x126ac | 0x6c8 | data | | |
| RT_ICON | 0x12d74 | 0x568 | GLS_BINARY_LSB_FIRST | | |
| RT_ICON | 0x132dc | 0x42028 | dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0 | | |
| RT_ICON | 0x55304 | 0x25a8 | data | | |
| RT_ICON | 0x578ac | 0x10a8 | data | | |
| RT_ICON | 0x58954 | 0x988 | data | | |
| RT_ICON | 0x592dc | 0x468 | GLS_BINARY_LSB_FIRST | | |
| RT_GROUP_ICON | 0x59744 | 0xbc | data | | |

## Network Behavior

### UDP Packets

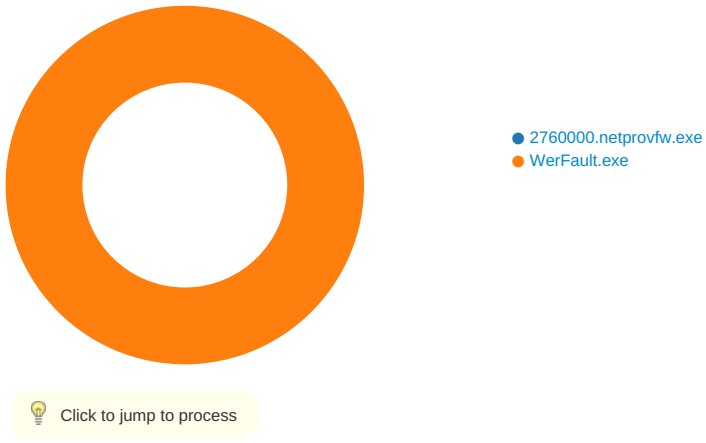
| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 28, 2021 16:27:44.950273991 CET | 63492 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:45.001044035 CET | 53 | 63492 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:45.804285049 CET | 60831 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:45.852279902 CET | 53 | 60831 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:46.676866055 CET | 60100 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:46.728919983 CET | 53 | 60100 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:47.529217005 CET | 53195 | 53 | 192.168.2.3 | 8.8.8.8 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 28, 2021 16:27:47.577835083 CET | 53 | 53195 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:48.344050884 CET | 50141 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:48.394737959 CET | 53 | 50141 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:49.204808950 CET | 53023 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:49.261265993 CET | 53 | 53023 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:50.005877018 CET | 49563 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:50.057293892 CET | 53 | 49563 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:50.848668098 CET | 51352 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:50.896701097 CET | 53 | 51352 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:51.791634083 CET | 59349 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:51.844265938 CET | 53 | 59349 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:52.679951906 CET | 57084 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:52.727832079 CET | 53 | 57084 | 8.8.8.8 | 192.168.2.3 |
| Jan 28, 2021 16:27:52.961210966 CET | 58823 | 53 | 192.168.2.3 | 8.8.8.8 |
| Jan 28, 2021 16:27:53.011951923 CET | 53 | 58823 | 8.8.8.8 | 192.168.2.3 |

# Code Manipulations

# Statistics

## Behavior




# System Behavior

## Analysis Process: 2760000.netprovfw.exe PID: 3636 Parent PID: 5668

### General

| | |
|---|---|
| Start time: | 16:27:50 |
| Start date: | 28/01/2021 |
| Path: | C:\Users\user\Desktop\2760000.netprovfw.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\2760000.netprovfw.exe' |
| Imagebase: | 0x2760000 |
| File size: | 350208 bytes |
| MD5 hash: | 90478BB3273D74A7A4BAE530DEE87174 |
| Has elevated privileges: | true |

Copyright null 2021

| | |
|---|---|
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.215311677.0000000002761000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.206372217.0000000002761000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | low |

## Analysis Process: WerFault.exe PID: 4852 Parent PID: 3636

### General

| | |
|---|---|
| Start time: | 16:27:51 |
| Start date: | 28/01/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 3636 -s 640 |
| Imagebase: | 0x1210000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

#### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\DBG | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 6E261717 | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp | read attributes \| synchronize \| generic read | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp | read attributes \| synchronize \| generic read | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81A.tmp | read attributes \| synchronize \| generic read | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81A.tmp.xml | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_2760000.netprovf_50482980db6f70d047bdd5f2b763ef22b1cfde7_9c33c211_129efdf4 | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_2760000.netprovf_50482980db6f70d047bdd5f2b763ef22b1cfde7_9c33c211_129efdf4\Report.wer | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 6E25497A | unknown |

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81A.tmp | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | success or wait | 1 | 6E254BEF | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | success or wait | 1 | 6E254BEF | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81A.tmp.xml | success or wait | 1 | 6E254BEF | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WER80C6.tmp.csv | success or wait | 1 | 6E254BEF | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WER80E6.tmp.txt | success or wait | 1 | 6E254BEF | unknown |

**File Written**

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 32 | 4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 88 56 13 60 a4 05 12 00 00 00 00 00 | MDMP..... .....V.`..... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 6 | 00 00 00 00 00 00 | ..... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 1420 | 00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 54 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 34 0e 00 00 86 56 13 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 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 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 | .....U.....B.....T..... ..GenuineIntelW.....T... ....4....V.`..... .....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..... | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 716 | 7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 6612 | bc 9a e5 77 a3 1a 21 75 aa aa aa aa 60 e8 19 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 7c 02 00 00 74 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 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\WERF5C6.tmp.dmp | unknown | 48 | 2a 00 00 00 32 00 37 00 36 00 30 00 30 00 30 00 30 00 2e 00 6e 00 65 00 74 00 70 00 72 00 6f 00 76 00 66 00 77 00 2e 00 65 00 78 00 65 00 00 00 | *...2.7.6.0.0.0.0...n.e.t.p.r.o.v.f.w...e.x.e... | success or wait | 36 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 752 | 00 00 12 74 00 00 00 00 00 f0 00 00 db 41 01 00 97 08 8a 7e 74 1d 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 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 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 85 02 00 00 00 00 00 a0 b0 02 00 00 00 00 fd 24 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 4e 49 03 00 00 00 00 00 b9 4b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 99 1b 00 00 00 00 00 26 66 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 49 dc 04 00 00 00 00 | ...t.....A.....~t.....B.....B?.....%.....@A.....Zb.....p.....$.....NI.....K.....&f.....@.....I..... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 9072 | 12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 | ....D.i.r.e.c.t.o.r.y.....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5C6.tmp.dmp | unknown | 108 | 03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 34 0f 00 00 9c 07 00 00 05 00 00 00 14 01 00 00 c2 28 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 10 19 00 00 36 8a 00 00 15 00 00 00 ec 01 00 00 d0 16 00 00 16 00 00 00 98 00 00 00 bc 18 00 00 | ................4.....(.....T.....8.....T.....6.....  | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | ff fe | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.?.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.".?.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.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.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.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.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.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.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.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.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.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.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.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.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 30 | 3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00 | <.P.i.d.>.3.6.3.6.<./.P.i.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 88 | 3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 32 00 37 00 36 00 30 00 30 00 30 00 30 00 30 00 2e 00 6e 00 65 00 74 00 70 00 72 00 6f 00 76 00 66 00 77 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 | <.I.m.a.g.e.N.a.m.e.>.2.7.6.0.0.0.0...n.e.t.p.r.o.v.f.w...e.x.e.<./.I.m.a.g.e.N.a.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 42 | 3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 37 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 | <.U.p.t.i.m.e.>.2.4.7.3.<./.U.p.t.i.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 82 | 3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00 | <.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 86 | 3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 38 00 39 00 33 00 32 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 | <.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.8.8.9.3.2.3.5.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 70 | 3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 38 00 39 00 32 00 34 00 31 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 | <.V.i.r.t.u.a.l.S.i.z.e.>.8.8.9.2.4.1.6.0.<./.V.i.r.t.u.a.l.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 74 | 3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 | <.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.3.3.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 39 00 30 00 38 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 | <.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.8.9.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 39 00 30 00 38 00 39 00 30 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 | <.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.8.9.0.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 36 00 38 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.8.8.5.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 36 00 38 00 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.8.6.9.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 32 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 | <.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.5.2.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.2.5.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 30 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.1.0.8.8.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 31 00 37 00 30 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.1.1.7.0.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 30 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.P.r.i.v.a.t.e.U.s.a.g.e.>.3.1.0.8.8.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.a.r.e.n.t.P.r.o.c.e.s.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 30 | 3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00 | <.P.i.d.>.3.3.8.8.<./.P.i.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 70 | 3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 | <.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 90 | 3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 | <.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 48 | 3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 30 00 38 00 35 00 35 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 | <.U.p.t.i.m.e.>.7.0.0.8.5.5.3.<./.U.p.t.i.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.W.o.w.6.4..g.u.e.s.t.=.".0.".h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 90 | 3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 | <.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 74 | 3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 | <.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 76 | 3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 36 00 30 00 30 00 30 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 | <.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.6.0.0.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 100 | 3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 31 00 30 00 33 00 39 00 33 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 | <.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.4.1.0.3.9.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 84 | 3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 37 00 36 00 38 00 30 00 36 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 | <.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.3.7.6.8.0.6.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 39 00 36 00 33 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.3.5.8.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 39 00 33 00 38 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.8.0.3.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 37 00 32 00 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.0.9.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 37 00 30 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.0.8.5.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 78 | 3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 30 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.9.0.6.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 94 | 3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 31 00 30 00 35 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.1.0.5.6.6.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 5 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 74 | 3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 30 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 | <.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.9.0.6.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 4 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.a.r.e.n.t.P.r.o.c.e.s.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 8 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 16 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 92 | 3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 32 00 37 00 36 00 30 00 30 00 30 00 30 00 2e 00 6e 00 65 00 74 00 70 00 72 00 6f 00 76 00 66 00 77 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 | <.P.a.r.a.m.e.t.e.r.0.>.2.7.6.0.0.0.0...n.e.t.p.r.o.v.f.w...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>. | success or wait | 8 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 6 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 12 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>. | success or wait | 6 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 106 | 3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 63 00 61 00 76 00 75 00 63 00 6d 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 | <.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.c.a.v.u.c.m.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 96 | 3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 61 00 76 00 75 00 63 00 6d 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 | <.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.c.a.v.u.c.m.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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 | <.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 35 00 36 00 30 00 33 00 35 00 36 00 31 00 37 00 35 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 | <.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.0.3.5.6.1.7.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.I.n.t.e.g.r.a.t.o.r.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 6 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00 | <.F.l.a.g.s.>.0.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>. | success or wait | 3 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.I.n.t.e.g.r.a.t.o.r.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 31 00 2d 00 30 00 31 00 2d 00 32 00 39 00 54 00 30 00 30 00 3a 00 32 00 37 00 3a 00 35 00 32 00 5a 00 22 00 3e 00 | <.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.2.9.T.0.0.:.2.7.:.5.2.Z.".>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 258 | 3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 36 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 | <.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.1.". .P.I.D.=.".3.6.3.6.". .U.p.t.i.m.e.M.S.=.".4.0.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.0.6.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1." | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 20 | 3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00 | <./.P.r.o.c.e.s.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 98 | 3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 64 00 65 00 39 00 64 00 66 00 31 00 33 00 2d 00 62 00 61 00 63 00 64 00 2d 00 34 00 61 00 61 00 62 00 2d 00 38 00 37 00 66 00 35 00 2d 00 61 00 33 00 37 00 31 00 31 00 64 00 62 00 35 00 30 00 30 00 36 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00 | <.G.u.i.d.>.4.d.e.9.d.f.1.3.-.b.a.c.d.-.4.a.a.b.-.8.7.f.5.-.a.3.7.1.1.d.b.5.0.0.6.1.<./.G.u.i.d.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 2 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 31 00 2d 00 30 00 31 00 2d 00 32 00 39 00 54 00 30 00 30 00 3a 00 32 00 37 00 3a 00 35 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 | <.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.2.9.T.0.0.:.2.7.:.5.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 2 | 09 00 | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 4 | 0d 00 0a 00 | .... | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF78C.tmp.WERInternalMetadata.xml | unknown | 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 | <./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>. | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\ProgramData\Microsoft\Windows\WER\Temp\WERF81A.tmp.xml | unknown | 4605 | 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22 | <?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val=" | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_2760000.netprovf_50482980db6f70d047bdd5f2b763ef22b1cfde7_9c33c211_129efdf4\Report.wer | unknown | 2 | ff fe | .. | success or wait | 1 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_2760000.netprovf_50482980db6f70d047bdd5f2b763ef22b1cfde7_9c33c211_129efdf4\Report.wer | unknown | 22 | 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00 | V.e.r.s.i.o.n.=.1..... | success or wait | 166 | 6E25497A | unknown |
| C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_2760000.netprovf_50482980db6f70d047bdd5f2b763ef22b1cfde7_9c33c211_129efdf4\Report.wer | unknown | 46 | 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 38 00 38 00 35 00 39 00 30 00 34 00 38 00 37 00 33 00 | M.e.t.a.d.a.t.a.H.a.s.h.=.-.8.8.5.9.0.4.8.7.3. | success or wait | 1 | 6E25497A | unknown |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Registry Activities

### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\PermissionsCheckTestKey | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\PermissionsCheckTestKey | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\ffdbf6c1 | success or wait | 1 | 6E2736BF | unknown |
| HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug | success or wait | 1 | 6E271FB2 | RegCreateKeyExW |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\PermissionsCheckTestKey | success or wait | 1 | 6E2543D1 | unknown |

### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\ffdbf6c1 | ProgramId | unicode | 0006d0fcc325598950a9bb8ca5b65891d6860000ffff | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\ffdbf6c1 | FileId | unicode | 00008fa8f069d4391a21346de65a5ee729ad6ef56a60 | success or wait | 1 | 6E2736BF | unknown |

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | LowerCaseLongPath | unicode | c:\users\user\desktop\2760000.netprovfw.exe | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | LongPathHash | unicode | 2760000.netprovf\|ffdbf6c1 | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | Name | unicode | 2760000.netprovfw.exe | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | Publisher | unicode | | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | Version | unicode | | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | BinFileVersion | unicode | | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | BinaryType | unicode | pe32_i386 | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | ProductName | unicode | | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | ProductVersion | unicode | | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | LinkDate | unicode | 10/21/2020 21:08:29 | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | BinProductVersion | unicode | | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | Size | B | 00 58 05 00 00 00 00 00 | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | Language | dword | 0 | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | IsPeFile | dword | 1 | success or wait | 1 | 6E2736BF | unknown |
| \REGISTRY\A\{6cd0de9c-2916-baae-bac4-52b827e3ef00}\Root\InventoryApplicationFile\2760000.netprovf\|ffdbf6c1 | IsOsComponent | dword | 0 | success or wait | 1 | 6E2736BF | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug | ExceptionRecord | binary | 05 00 00 C0 00 00 00 00 00 00 00 00 04 3D 4F 76 02 00 00 00 01 00 00 00 B8 FF FF FF 00 00 00 00 00 00 00 00