ID: 357080
Sample Name: Payment Advice 80642111.exe
Cookbook: default.jbs
Time: 07:26:13
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Payment Advice 80642111.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: HawkEye 5
Yara Overview 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 6
Signature Overview 6
AV Detection: 7
Compliance: 7
Key, Mouse, Clipboard, Microphone and Screen Capturing: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
URLs from Memory and Binaries 12
Contacted IPs 18
Public 18
Private 18
General Information 18
Simulations 20
Behavior and APIs 20
Joe Sandbox View / Context 21
IPs 21
Domains 21
ASN 21
JA3 Fingerprints 22
Dropped Files 22
Created / dropped Files 22
Static File Info 27
General 27
File Icon 27
Static PE Info 27
General 27

Entrypoint Preview 27
Data Directories 29
Sections 29
Resources 29
Imports 30
Version Infos 30
Network Behavior 30
Network Port Distribution 30
TCP Packets 30
UDP Packets 31
DNS Queries 32
DNS Answers 32
SMTP Packets 32
Code Manipulations 32
Statistics 33
Behavior 33
System Behavior 33
Analysis Process: Payment Advice 80642111.exe PID: 6428 Parent PID: 5748 33
General 33
File Activities 33
File Created 33
File Written 34
File Read 34
Analysis Process: Payment Advice 80642111.exe PID: 6464 Parent PID: 6428 34
General 35
Analysis Process: Payment Advice 80642111.exe PID: 6488 Parent PID: 6428 35
General 35
Analysis Process: Payment Advice 80642111.exe PID: 6496 Parent PID: 6428 35
General 35
Analysis Process: Payment Advice 80642111.exe PID: 6508 Parent PID: 6428 35
General 35
File Activities 36
File Created 36
File Written 37
File Read 37
Registry Activities 38
Key Value Created 38
Key Value Modified 38
Analysis Process: vbc.exe PID: 7116 Parent PID: 6508 38
General 38
Analysis Process: vbc.exe PID: 7124 Parent PID: 6508 38
General 38
Analysis Process: WerFault.exe PID: 3220 Parent PID: 7116 38
General 39
File Activities 39
File Created 39
File Deleted 39
File Written 39
Registry Activities 61
Key Created 61
Key Value Created 61
Analysis Process: WerFault.exe PID: 204 Parent PID: 7124 62
General 62
File Activities 62
File Created 62
File Deleted 62
File Written 63
Registry Activities 85
Key Created 85
Key Value Created 85
Key Value Modified 86
Analysis Process: WindowsUpdate.exe PID: 5480 Parent PID: 3472 86
General 86
File Activities 87
File Created 87
File Written 87
File Read 88
Analysis Process: WindowsUpdate.exe PID: 6228 Parent PID: 5480 88
General 88
File Activities 89
File Created 89
File Deleted 89
File Written 89
File Read 90

Analysis Process: WindowsUpdate.exe PID: 804 Parent PID: 3472 90
General 90
Analysis Process: WindowsUpdate.exe PID: 6992 Parent PID: 804 91
General 91
Analysis Process: vbc.exe PID: 6452 Parent PID: 6228 91
General 91
Analysis Process: vbc.exe PID: 6876 Parent PID: 6228 92
General 92
Disassembly 92
Code Analysis 92

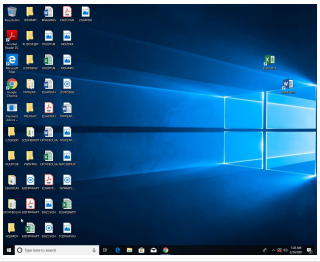
Analysis Report Payment Advice 80642111.exe

Overview

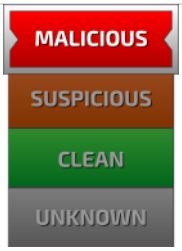
General Information

Sample Name:	Payment Advice 80642111.exe
Analysis ID:	357080
MD5:	85bd30d4211b1d..
SHA1:	74fdf25bef9f31e3..
SHA256:	6f2af9503a84bf2…
Tags:	exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



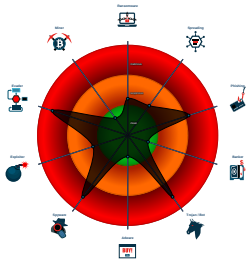
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Binary contains a suspicious time st…
- Changes the view of files in windows…
- Contains functionality to log keystro…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- Payment Advice 80642111.exe (PID: 6428 cmdline: 'C:\Users\user\Desktop\Payment Advice 80642111.exe' MD5: 85BD30D4211B1DFF2FE6847502341831)
  - Payment Advice 80642111.exe (PID: 6464 cmdline: C:\Users\user\Desktop\Payment Advice 80642111.exe MD5: 85BD30D4211B1DFF2FE6847502341831)
  - Payment Advice 80642111.exe (PID: 6488 cmdline: C:\Users\user\Desktop\Payment Advice 80642111.exe MD5: 85BD30D4211B1DFF2FE6847502341831)
  - Payment Advice 80642111.exe (PID: 6496 cmdline: C:\Users\user\Desktop\Payment Advice 80642111.exe MD5: 85BD30D4211B1DFF2FE6847502341831)
  - Payment Advice 80642111.exe (PID: 6508 cmdline: C:\Users\user\Desktop\Payment Advice 80642111.exe MD5: 85BD30D4211B1DFF2FE6847502341831)
    - vbc.exe (PID: 7116 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - WerFault.exe (PID: 3220 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7116 -s 176 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - vbc.exe (PID: 7124 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
      - WerFault.exe (PID: 204 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 176 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- WindowsUpdate.exe (PID: 5480 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: 85BD30D4211B1DFF2FE6847502341831)
  - WindowsUpdate.exe (PID: 6228 cmdline: C:\Users\user\AppData\Roaming\WindowsUpdate.exe MD5: 85BD30D4211B1DFF2FE6847502341831)
    - vbc.exe (PID: 6452 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6876 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- WindowsUpdate.exe (PID: 804 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: 85BD30D4211B1DFF2FE6847502341831)
  - WindowsUpdate.exe (PID: 6992 cmdline: C:\Users\user\AppData\Roaming\WindowsUpdate.exe MD5: 85BD30D4211B1DFF2FE6847502341831)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView",
    "mailpv",
    "Mail PassView"
  ],
  "Version": ""
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001C.00000002.346347222.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000004.00000002.283540022.00000000039A4000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000004.00000002.293943590.000000000850000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000004.00000002.278382516.000000000293000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000004.00000002.278382516.000000000293000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x39848:$hawkstr1: HawkEye Keylogger • 0x3cd6c:$hawkstr1: HawkEye Keylogger • 0x3d148:$hawkstr1: HawkEye Keylogger • 0x41d4c:$hawkstr1: HawkEye Keylogger • 0x1452f0:$hawkstr1: HawkEye Keylogger • 0x39300:$hawkstr2: Dear HawkEye Customers! • 0x3cdcc:$hawkstr2: Dear HawkEye Customers! • 0x3d1a8:$hawkstr2: Dear HawkEye Customers! • 0x3942e:$hawkstr3: HawkEye Logger Details:
Click to see the 68 entries				

Unpacked PEs

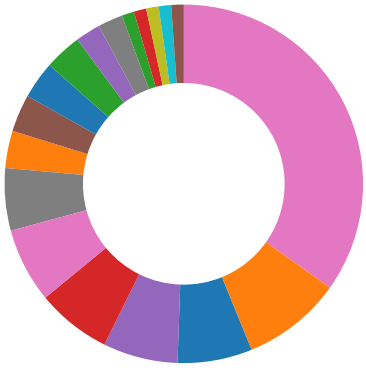
Source	Rule	Description	Author	Strings
4.2.Payment Advice 80642111.exe.400000.0.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
4.2.Payment Advice 80642111.exe.400000.0.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b90f:$key: HawkEyeKeylogger • 0x7db45:$salt: 099u787978786 • 0x7bf1c:$string1: HawkEye_Keylogger • 0x7cd6f:$string1: HawkEye_Keylogger • 0x7daa5:$string1: HawkEye_Keylogger • 0x7c305:$string2: holdermail.txt • 0x7c325:$string2: holdermail.txt • 0x7c247:$string3: wallet.dat • 0x7c25f:$string3: wallet.dat • 0x7c275:$string3: wallet.dat • 0x7d687:$string4: Keylog Records • 0x7d99f:$string4: Keylog Records • 0x7db9d:$string5: do not script --> • 0x7b8f7:$string6: \pidloc.txt • 0x7b951:$string7: BSPLIT • 0x7b961:$string7: BSPLIT
4.2.Payment Advice 80642111.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
4.2.Payment Advice 80642111.exe.400000.0.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
4.2.Payment Advice 80642111.exe.400000.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 158 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance



- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger
- Contains functionality to log keystrokes (.Net Source)

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker
- Binary contains a suspicious time stamp
- Yara detected Beds Obfuscator

Hooking and other Techniques for Hiding and Protection:

- Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

- Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions
- Injects a PE file into a foreign processes
- Sample uses process hollowing technique
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Instant Messenger accounts or passwords
- Tries to steal Mail credentials (via file access)
- Yara detected WebBrowserPassView password recovery tool

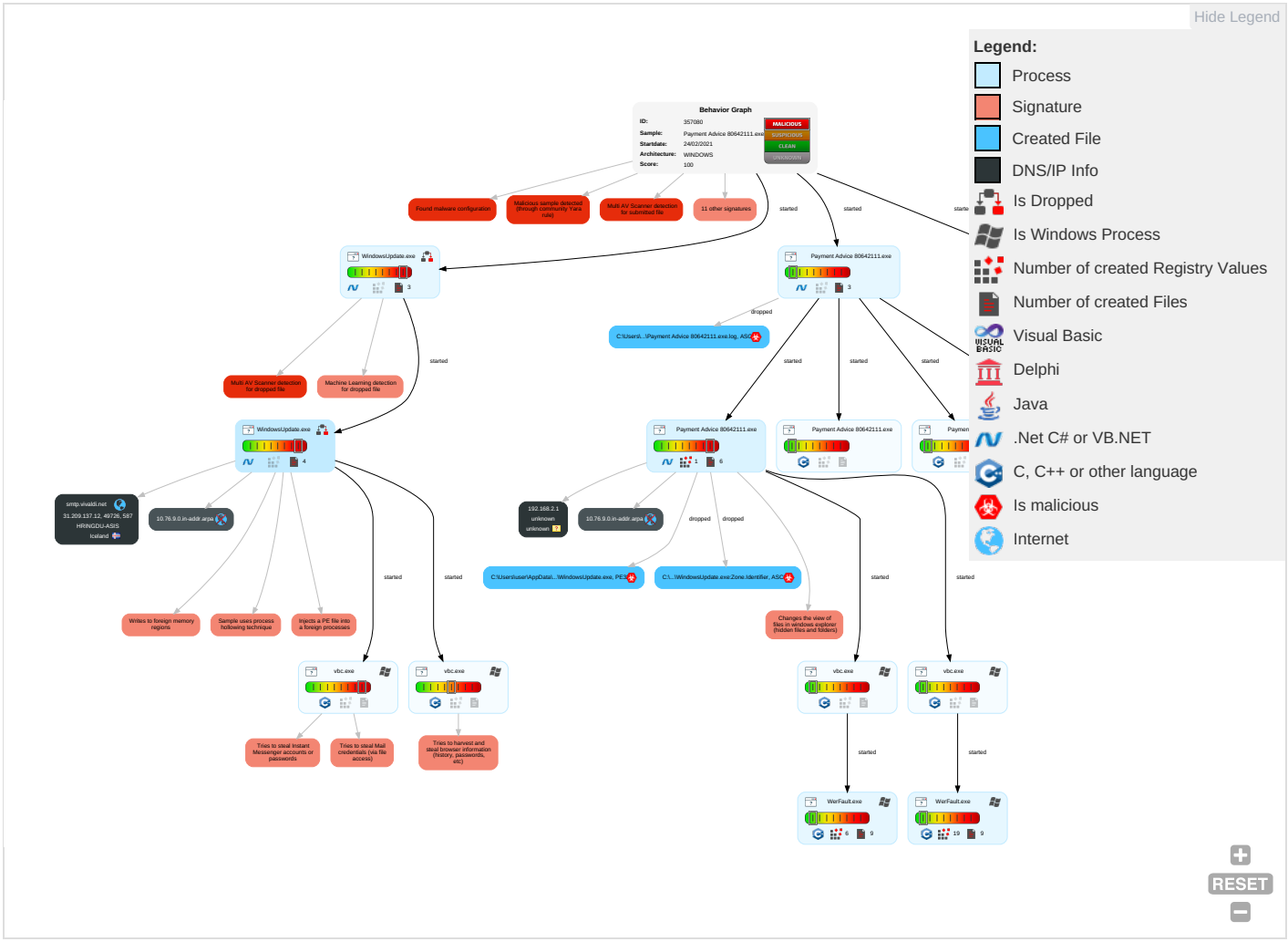
Remote Access Functionality:

- Detected HawkEye Rat
- Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Disable or Modify Tools 1	OS Credential Dumping 1	Peripheral Device Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 5	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Remote Acce Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	Credentials In Files 1	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

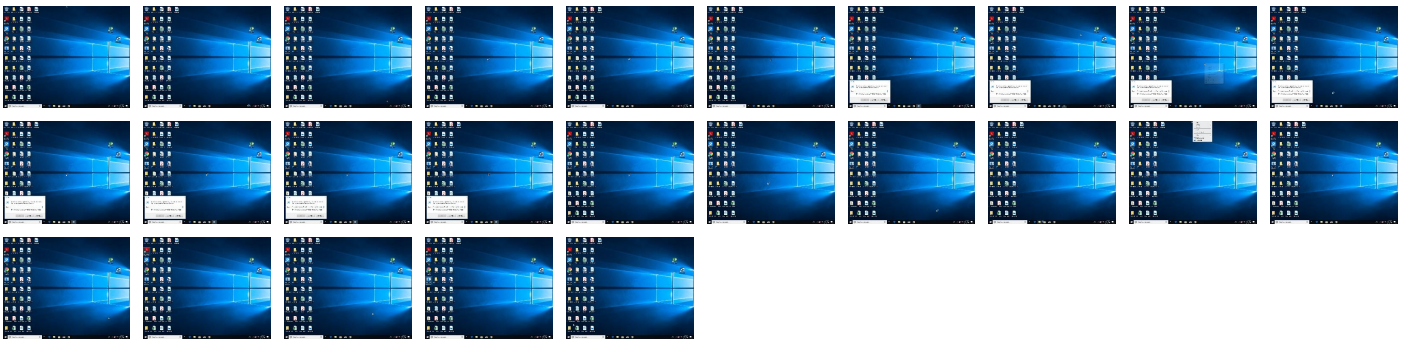
Behavior Graph



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
Payment Advice 80642111.exe	61%	Virustotal		Browse
Payment Advice 80642111.exe	24%	Metadefender		Browse
Payment Advice 80642111.exe	68%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Payment Advice 80642111.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	68%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Payment Advice 80642111.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
4.2.Payment Advice 80642111.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
23.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
23.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
27.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
27.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
28.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
4.2.Payment Advice 80642111.exe.296f4cc.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

Source	Detection	Scanner	Label	Link
10.76.9.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Ky	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/yy	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/gy	0%	Avira URL Cloud	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Jy	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cny	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicryz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/staff/dennis.htmh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/gy	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//(	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://foo.com/foo	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Ty	0%	Avira URL Cloud	safe	
http://cps.root	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.vivaldi.net	31.209.137.12	true	false		high
10.76.9.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/?	Payment Advice 80642111.exe, 00000004.00000003.238665028.0000005AF9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.p	vbc.exe, 0000001C.00000002.346657064.000000000061D000.00000004.00000020.sdmp	false		high
http://www.fontbureau.com/designers/?	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.microsoft	WindowsUpdate.exe, 00000017.00000002.507254853.0000000007097000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/?ocid=iehpLMEMh	vbc.exe, 0000001C.00000002.346625388.0000000000608000.00000004.00000020.sdmp	false		high
http://www.fontbureau.com/designers?	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Ky	Payment Advice 80642111.exe, 00000004.00000003.238665028.0000005AF9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersY	Payment Advice 80642111.exe, 00000004.00000003.240736289.0000005B2E000.00000004.00000001.sdmp	false		high
http://www.tiro.com	WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://blog.naver.com/cubemit314Ghttp://projectofsonagi.tistory.com/	Payment Advice 80642111.exe, 00000000.00000002.232301416.00000039D9000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000015.00000002.303042650.000037F9000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000001A.00000002.318746225.0000003FA9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnF	Payment Advice 80642111.exe, 00000004.00000003.236653540.0000005B1E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/yy	Payment Advice 80642111.exe, 00000004.00000003.237769137.0000005AF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/B	Payment Advice 80642111.exe, 00000004.00000003.240153326.0000005B2E000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/gy	Payment Advice 80642111.exe, 00000004.00000003.238081922.0000005AFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersN	Payment Advice 80642111.exe, 00000004.00000003.242522578.0000005B2E000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comI1	Payment Advice 80642111.exe, 00000004.00000002.287976818.0000005AFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	WindowsUpdate.exe, 00000017.00000003.366717151.00000000035F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Payment Advice 80642111.exe, 00000004.00000003.243159760.0000005B21000.00000004.00000001.sdmp, Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Payment Advice 80642111.exe, 00000004.00000003.235761615.0000005AFD000.00000004.00000001.sdmp, Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	Payment Advice 80642111.exe, 00000004.00000003.237769137.0000005AF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	vbc.exe, 0000001C.00000003.345554125.000000000092C000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Jy	Payment Advice 80642111.exe, 00000004.00000003.238081922.0000005AFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	vbc.exe, 0000001C.00000003.345554125.000000000092C000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cny	Payment Advice 80642111.exe, 00000004.00000003.237023942.0000005AFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnicryz	Payment Advice 80642111.exe, 00000004.00000003.237023942.0000005AFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

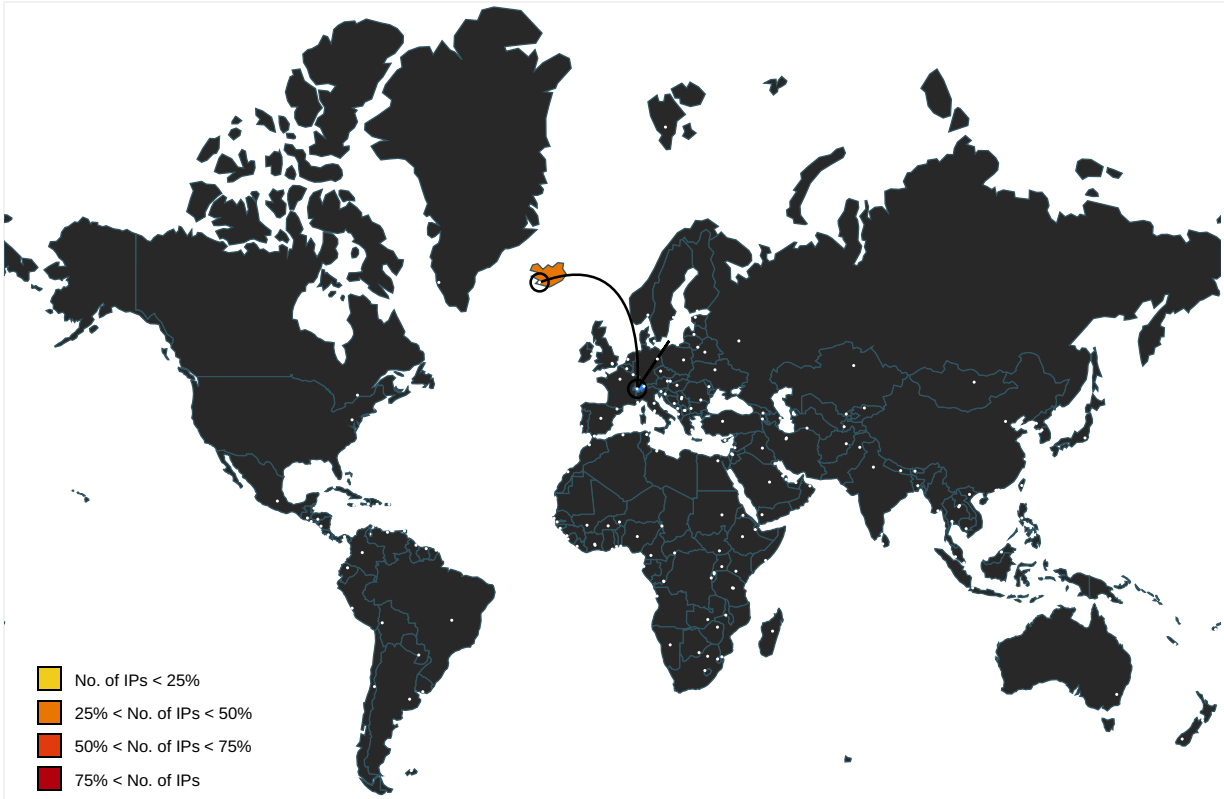
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/-	Payment Advice 80642111.exe, 00000004.00000003.238081922.0000005AFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehp	vbc.exe, 0000001C.00000002.346625388.0000000000608000.00000004.00000020.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmh	Payment Advice 80642111.exe, 00000004.00000003.243159760.0000005B21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	Payment Advice 80642111.exe, 00000000.00000002.232301416.00000039D9000.00000004.00000001.sdmp, Payment Advice 80642111.exe, 00000004.00000002.275693727.0000000000402000.00000040.00000001.sdmp, WindowsUpdate.exe, 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.488882188.0000000000402000.00000040.00000001.sdmp, WindowsUpdate.exe, 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000001B.00000002.321590143.0000000000402000.00000040.00000001.sdmp	false		high
http://www.fontbureau.com/designersb	Payment Advice 80642111.exe, 00000004.00000003.242522578.0000005B2E000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/gy	Payment Advice 80642111.exe, 00000004.00000003.238336955.0000005AF5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	WindowsUpdate.exe, 00000017.00000003.366717151.00000000035F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersx	Payment Advice 80642111.exe, 00000004.00000003.242433196.0000005B2E000.00000004.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	Payment Advice 80642111.exe, 00000004.00000003.238762251.0000005B2C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	Payment Advice 80642111.exe, 00000004.00000002.278382516.0000002931000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.495351637.00000002D21000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1https://c	vbc.exe, 0000001C.00000003.345554125.000000000092C000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	vbc.exe, 0000001D.00000002.343283889.0000000000400000.00000040.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/checksync.phphttps://contextual.media.net/checksync.php?&vsSync=1&cs=1&	vbc.exe, 0000001C.00000003.345554125.000000000092C000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment Advice 80642111.exe, 00000004.00000002.278382516.0000002931000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.495351637.0000002D21000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000001B.00000002.327611606.00000000033F1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	WindowsUpdate.exe, 00000017.00000003.366717151.00000000035F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false		high
http://cps.letsencrypt.org0	WindowsUpdate.exe, 00000017.00000003.366717151.00000000035F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//(	Payment Advice 80642111.exe, 00000004.00000003.237769137.0000005AF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Payment Advice 80642111.exe, 00000004.00000003.238081922.0000005AFA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	Payment Advice 80642111.exe, 00000004.00000002.287976818.0000005AFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/?	Payment Advice 80642111.exe, 00000004.00000003.237769137.0000005AF4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://foo.com/foo	WindowsUpdate.exe, 0000001B.00000002.327611606.00000000033F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/z	Payment Advice 80642111.exe, 00000004.00000003.238081922.0000005AFA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Ty	Payment Advice 80642111.exe, 00000004.00000003.238665028.0000005AF9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root	WindowsUpdate.exe, 00000017.00000002.507092380.0000000007036000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Payment Advice 80642111.exe, 00000004.00000003.236783840.0000005B1E000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://crl.micro	WerFault.exe, 00000012.00000003.320829363.0000000000A33000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnt;	Payment Advice 80642111.exe, 00000004.00000003.237023942.0000005AFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/Ty	Payment Advice 80642111.exe, 00000004.00000003.238081922.0000005AFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Payment Advice 80642111.exe, 00000004.00000003.237769137.0000005AF4000.00000004.00000001.sdmp, Payment Advice 80642111.exe, 00000004.00000003.238081922.00000005AFA000.00000004.00000001.sdmp, Payment Advice 80642111.exe, 00000004.00000003.238665028.0000000005AF9000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.0000000005EE0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comN	Payment Advice 80642111.exe, 00000004.00000003.237013015.0000005B1E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/i	Payment Advice 80642111.exe, 00000004.00000003.238665028.0000005AF9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Payment Advice 80642111.exe, 00000004.00000002.288048178.0000005BE0000.00000002.00000001.sdmp, WindowsUpdate.exe, 00000017.00000002.506391942.00000005EE0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/fr-c	Payment Advice 80642111.exe, 00000004.00000003.238665028.0000005AF9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=(	vbc.exe, 0000001C.00000002.346657064.000000000061D000.00000004.00000020.sdmp	false		high
http://https://login.microsoftonline.com/common/oauth2/TT	vbc.exe, 0000001C.00000002.346657064.000000000061D000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html8G	Payment Advice 80642111.exe, 00000004.00000003.241248337.0000005B2E000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	Payment Advice 80642111.exe, 00000004.00000003.240153326.0000005B2E000.00000004.00000001.sdmp	false		high
http://r3.i.lencr.org/0f	WindowsUpdate.exe, 00000017.000000002.507092380.0000000007036000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.209.137.12	unknown	Iceland		51896	HRINGDU-ASIS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357080
Start date:	24.02.2021
Start time:	07:26:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 50s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	Payment Advice 80642111.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@25/17@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 71% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 51.103.5.159, 13.64.90.137, 204.79.197.200, 13.107.21.200, 93.184.220.29, 51.104.144.132, 92.122.145.220, 104.43.193.48, 40.88.32.150, 23.218.208.56, 104.42.151.234, 52.255.188.83, 51.103.5.186, 8.253.95.249, 8.248.147.254, 8.253.95.121, 8.248.115.254, 8.248.145.254, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:27:18	API Interceptor	4x Sleep call for process: Payment Advice 80642111.exe modified
07:27:21	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
07:27:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
07:27:45	API Interceptor	2x Sleep call for process: WerFault.exe modified
07:27:47	API Interceptor	37x Sleep call for process: WindowsUpdate.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.209.137.12	Invoice from GQH CO.,LTD (683814).exe	Get hash	malicious	Browse	
	EFECO SAUDI LLC -NEW OFFER #210218.exe	Get hash	malicious	Browse	
	invoice.jpg.scr.exe	Get hash	malicious	Browse	
	PO #047428.exe	Get hash	malicious	Browse	
	Scanned from PNB Sales Office Copier.pdf.exe	Get hash	malicious	Browse	
	NEW ORDER INQUIRY_B1020289.pdf.exe	Get hash	malicious	Browse	
	PO #047428.exe	Get hash	malicious	Browse	
	Quote JQ102474.pdf.exe	Get hash	malicious	Browse	
	Quotation Sheet and PO CARESCAPE R860 Ventilator.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	air ventilation systems_temperature 20-25 #U00b0.exe	Get hash	malicious	Browse	
	QUOTE B1020363.pdf.exe	Get hash	malicious	Browse	
	ABB offer 02.5.2021.abb.pdf.exe	Get hash	malicious	Browse	
	Archived.doc.exe	Get hash	malicious	Browse	
	24906_technical_datas.exe	Get hash	malicious	Browse	
	PO #047428.exe	Get hash	malicious	Browse	
	SWIFT_876544.exe	Get hash	malicious	Browse	
	MT103_001.exe	Get hash	malicious	Browse	
	MT103_001.exe	Get hash	malicious	Browse	
	NEW ORDER FROM AUTONOLOGY CO.,LIMITED_PO #7A68D20.pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.vivaldi.net	Invoice from GQH CO.,LTD (683814).exe	Get hash	malicious	Browse	• 31.209.137.12
	EFECO SAUDI LLC -NEW OFFER #210218.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.jpg.scr.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO #047428.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scanned from PNB Sales Office Copier.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	NEW ORDER INQUIRY_B1020289.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO #047428.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quote JQ102474.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotation Sheet and PO CARESCAPE R860 Ventilator.exe	Get hash	malicious	Browse	• 31.209.137.12
	New Order.exe	Get hash	malicious	Browse	• 31.209.137.12
	air ventilation systems_temperature 20-25 #U00b0.exe	Get hash	malicious	Browse	• 31.209.137.12
	QUOTE B1020363.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	ABB offer 02.5.2021.abb.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	Archived.doc.exe	Get hash	malicious	Browse	• 31.209.137.12
	24906_technical_datas.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO #047428.exe	Get hash	malicious	Browse	• 31.209.137.12
	SWIFT_876544.exe	Get hash	malicious	Browse	• 31.209.137.12
	MT103_001.exe	Get hash	malicious	Browse	• 31.209.137.12
	MT103_001.exe	Get hash	malicious	Browse	• 31.209.137.12
	NEW ORDER FROM AUTONOLOGY CO.,LIMITED_PO #7A68D20.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HRINGDU-ASIS	Invoice from GQH CO.,LTD (683814).exe	Get hash	malicious	Browse	• 31.209.137.12
	EFECO SAUDI LLC -NEW OFFER #210218.exe	Get hash	malicious	Browse	• 31.209.137.12
	invoice.jpg.scr.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO #047428.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scanned from PNB Sales Office Copier.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	NEW ORDER INQUIRY_B1020289.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO #047428.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quote JQ102474.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotation Sheet and PO CARESCAPE R860 Ventilator.exe	Get hash	malicious	Browse	• 31.209.137.12
	New Order.exe	Get hash	malicious	Browse	• 31.209.137.12

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	air ventilation systems_temperature 20-25 #U00b0.exe	Get hash	malicious	Browse	• 31.209.137.12
	QUOTE B1020363.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	ABB offer 02.5.2021.abb.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	Archived.doc.exe	Get hash	malicious	Browse	• 31.209.137.12
	24906_technical_datas.exe	Get hash	malicious	Browse	• 31.209.137.12
	PO #047428.exe	Get hash	malicious	Browse	• 31.209.137.12
	SWIFT_876544.exe	Get hash	malicious	Browse	• 31.209.137.12
	MT103_001.exe	Get hash	malicious	Browse	• 31.209.137.12
	MT103_001.exe	Get hash	malicious	Browse	• 31.209.137.12
	NEW ORDER FROM AUTONOLOGY CO.,LIMITED_PO #7A68D20.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f089e1f5158893287601d79f3806df6ebd7720_6c16ead4_0084324c\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7826
Entropy (8bit):	3.7667017788295856
Encrypted:	false
SSDEEP:	192:QCLqKDI0HJdmhf9jY/u7s7S274ltE7GDBF:TpD7JdmTjY/u7s7X4ltEOj
MD5:	FEA8FB37352748ABF52EEDDC1BAFD3AF
SHA1:	C0EB23FC2D3C423475CA4EBF40BB97ED85746274
SHA-256:	EB5EC84A3956D61FCA0FAFB9D3FB01251B7B3F60FB2AAE8739702C1E90505FD5
SHA-512:	14434C176FA25372FAD0B15EC14F0B7F5C8C4350320EFC39ACD71F29647C698C5559B5A3FD1D3A7D5DB15EBCA1E0C6AA04CAE19A206917A6BD09075BF3F2F88
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.=.1.3.2.5.8.6.5.4.0.4.9.7.5.1.0.4.2.6.....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.=.1.3.2.5.8.6.5.4.0.6.5.6.4.1.6.5.2.3.....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.l.d.e.n.t.i.f.i.e.r.=.2.b.3.4.5.3.a.9.-.0.8.b.5.-.4.a.3.b.-.b.f.d.9.-.e.8.b.e.6.c.a.6.2.4.e.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.1.6.d.7.5.a.5.-.9.3.f.e.-.4.8.4.e.-.8.8.0.2.-.7.6.7.b.2.4.9.0.4.9.5.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.v.b.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.v.b.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.d.4.-.0.0.0.1.-.0.0.1.6.-.9.c.f.a.-.7.8.8.c.c.1.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.7.8.7.d.9.a.6.e.c.3.f.2.6.2.e.8.b.7.1.d.1.9.a.c.1.5.7.c.2.a.2.8.6.a.0.f.5.9.d.d.!.v.b.c.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7824
Entropy (8bit):	3.767791835512396
Encrypted:	false
SSDEEP:	192:/d8VKUi2ymHBUZMXQf9jY/u7s7S274ltE7GDC:60Ui2TBUZMXojY/u7s7X4ltEOC
MD5:	16669F3D89747BE390D6EB5D1DCD21A5
SHA1:	91E77D1EB35104257E95B90952AD763E8653AF8F
SHA-256:	D9483646A43227D7D53CD46C17E667B34D3CEA36021FE51E6F2A3E6AF6EAEFC6
SHA-512:	E0BA77550BFDB1366453ACDD7C5E97923F50332C3610897E7FADD9517E32AE67319EFFD7143D188317CA5D19D9B312B5369F6F0171A8BAEE3B96748C190029C
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada\Report.wer	
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.=.1.3.2.5.8.6.5.4.0.4.9.1.3.9.2.6.3.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.6.5.4.0.6.3.0.9.4.7.7.7.9.....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.=.3.0.c.8.1.e.4.7.-.5.e.1.b.-.4.9.3.4.-.8.c.c.5.-.8.c.3.c.1.b.1.d.4.9.7.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.a.2.4.9.4.e.3.-.2.5.d.c.-.4.4.5.7.-.b.e.5.3.-.d.9.f.0.3.d.6.e.3.7.d.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.v.b.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.v.b.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.c.c.-.0.0.0.1.-.0.0.1.6.-.2.b.c.a.-.7.8.8.c.c.1.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.7.8.7.d.9.a.6.e.c.3.f.2.6.2.e.8.b.7.1.d.1.9.a.c.1.5.7.c.2.a.2.8.6.a.0.f.5.9.d.d.!.v.b.c.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 24 15:27:29 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	17690
Entropy (8bit):	2.246227175268669
Encrypted:	false
SSDEEP:	96:5Sw6l8Q/sJy8jAxSmXAwO39BYbQ5ih1UnWInWIXml4uH2C:4s48ExlA3tBeY01JuH2C
MD5:	AD181CBD689B1087A79DB8BC0A0F4AC7
SHA1:	2C57406A19B726584396FD393ADE18627E64103D
SHA-256:	EB57A20CEAACD4E1C804C7405D9F6B635F127E34DE5539E53B2BBBCCEB2FE80A
SHA-512:	C3DC62A49FECB327E85E71D1339182499E44DF723D9F4CDDB93C22E9EAB939066266E7D4902F8B3E2342509000C21FC4EF967745D9CF2E7992CFADA2126BDE
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....ap6`.....U.....B.....t.....GenuineIntelW.....T.....[p6`.....0..2.....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\WEREC2B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 24 15:27:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	17690
Entropy (8bit):	2.252376513132558
Encrypted:	false
SSDEEP:	96:5wu1l8Q//ZpDDmXADJF+28J+fDHa2ihGWHWInWIXml4zH1T:jxpDiAtFKJ+rL0HazH1T
MD5:	2D63378C69ADE33028F915A90B9C547B
SHA1:	89747F12FAFA86497032CC6569A4DB7E0C6EA0D7
SHA-256:	01DF1492A1F149CB981962B6843B78FBF720A6FA26A21EBBD12A4B4AB1F0F549
SHA-512:	276207F97628E9D3969E04EC186D69098044A2668AFEAB514D8B1EAA5AECE5C67AB7824DF88BCDC810A8DF1CA953115D6B6DD5F40586EFA15F12D4B01E3AEFD6
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....bp6`.....U.....B.....t.....GenuineIntelW.....T.....[p6`.....0..2.....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\WEREC5B.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):	3.7035939481039297
Encrypted:	false
SSDEEP:	192:RrI7r3GLNivV6CM6YFb6Regmf5sSU3CprT89bQ4qsf4WOm:RrlsNi96x6YJ6lgmf+SUrQ4JfNX
MD5:	11BC68309D5AC81A44B22BD76CCCCC63
SHA1:	6B55392DF74BA0C762ED683DAEFDD2E3BD9B9E1B
SHA-256:	110383C38453AF1AB3863AE63F30103C8F66F59991F1A2E5F434FA4F5FFAE56E
SHA-512:	EB29F9F17FE35C3593BA559FE895F310CBE0C43DDD7D0C3629E4F0C89942B812DC35FD22724C1ECA506CD9407BE753700822E9EA580918CE3BC5C9F14BA5239
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4643
Entropy (8bit):	4.480879266928618
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9r7WSC8BZ8fm8M4JzzZFG+q8jDYUlu5nNd:uITfiMKSNcJfSQHlu5nNd
MD5:	1B69D72770E23517194A87BAA694BA9E
SHA1:	179817EB40A5DEDBED8E767FF0FEF8E505193DAF
SHA-256:	25BE65318011103BD94ACA3A259E96BDD0F193A77A10584CA24DBE5390F24907
SHA-512:	8DC11825F2EA89CBB15FF25B3EF1866E6C898961D035079A37C1EFC6FBA71B9154A43C43CB1150E5393239DAFE60FB94A3E48AF9DB8C74124848E9894E30E25
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="875558" />.. <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" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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):	8320
Entropy (8bit):	3.701478060799241
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiGs6UvO6YF66Ogmf5CSY3Cprn89bQBasfSWRm:RrlsNit6N6YI6OgmfYSY3QB5fDs
MD5:	0F036666EAA82EFDC5BBE33C7F762561
SHA1:	E6FD8507D1FB425C6B66F03673A2157750FA1FB9
SHA-256:	0716AF1B62E45B1FED8E9A94D267EFE001091650353A6A806E270E00260D2F95
SHA-512:	64BEF5F5A3889B242ACA6FAAF86274734DF236C382151DEDD1958C9CED41FC2AE1551D7DA73F7D86FCF30F4C381E0D31FFA03E84C64618A6568A1ED60E2C6F0
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.>.7.1.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4643
Entropy (8bit):	4.4848666356737485
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9r7WSC8Bo8fm8M4JlRZF1I+q8vDxUlMScd:uITfiMKSN3JfK4alTcd
MD5:	D31A275CA1BE98D708626854C30B9D65
SHA1:	31172763FF260582AAE1AC57F7EB1E1A02E3232E
SHA-256:	78BAB11A900AB9394678E8892B9E501E871A93EFE18DB3AB4CBADCD791E997CE
SHA-512:	1AF3D829E1CB46D27EB7215FEBA25F658498B0DB7E03223EA5A6944C8D273FFB2903E9C2A9922FA89D94F34D8BB22EE41B2103E36635B7FA3F7F8F1C495601D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp.xml	
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="875558" />.. <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" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Advice 80642111.exe.log	
Process:	C:\Users\user\Desktop\Payment Advice 80642111.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCq1KDLI4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4Kx1qE4qpE4Ks2wKDE4KhK3VZ9px
MD5:	34580C7C598E15B8A008C82FE6A07CDF
SHA1:	2C90E9B7F4AFFE8FC7F9C313B4B867DF5B96CAC1
SHA-256:	08246B9BE1C37F8977CE083319A9D34BE09C65B926CBA30A5E062D79D5A4F1D6
SHA-512:	D836A862804608C3A127BF0CD30ECFB428E682D5E73D90C4C2837F93F02F12307F242F47F3CBBD71249AA6E608AFE230527F2F7D306A35A681346F9DDFE9D820
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WindowsUpdate.exe.log	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCq1KDLI4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4Kx1qE4qpE4Ks2wKDE4KhK3VZ9px
MD5:	34580C7C598E15B8A008C82FE6A07CDF
SHA1:	2C90E9B7F4AFFE8FC7F9C313B4B867DF5B96CAC1
SHA-256:	08246B9BE1C37F8977CE083319A9D34BE09C65B926CBA30A5E062D79D5A4F1D6
SHA-512:	D836A862804608C3A127BF0CD30ECFB428E682D5E73D90C4C2837F93F02F12307F242F47F3CBBD71249AA6E608AFE230527F2F7D306A35A681346F9DDFE9D820
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\Desktop\Payment Advice 80642111.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Size (bytes):	744448
Entropy (8bit):	**7.991542962307303**
Encrypted:	**true**
SSDEEP:	12288:xR/SQVieUU3JGNECPXYjy7cBwUpyRsMd1B4w4wpHr+26W5mc5ubo7qkdUmTAZnrh:xR/SQVi7U3JGNfPIjLqUp7Md7ZHpR53r
MD5:	85BD30D4211B1DFF2FE6847502341831
SHA1:	74FDF25BEF9F31E311B21D8CA572F834D03134C0
SHA-256:	6F2AF9503A84BF2C99E0BBF735B953A7551F7FF78F87C9AD84E8AFF091F2AE10
SHA-512:	EBB2DB3BF9315BFD4B307E587DA544471512E56CC6B3414E6BCD4F48E65C1D27C3AEBD16AC016794E9A540D11A7B1ADBB233B4D4C0267E901FD0BAAC9341FC4E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 68%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!(b.....0..R.....p... .....@.. ....@.....p..O..... ....H.....text....P... ...R..... ..`.rsrc.....T.....@..@.rel oc.....Z.....@..B.....p.....H.....Q.....5...$..."..... ".(.....*.(.....*~.|....(...-..|....(.....+..*..(....-.~ ...+..|....(.....|....(....s!...*..(....-.~ ...+..|....(.....|....(....s!...*..(....-..+..|....(.....|....(....Y*..|....(.....|....(.....(....s"...*z.~ ...}.....~ ...}.....(.....*..{....~....Y.{....~....Y~....~....s"...*r....(....}.....(....}....*..{....*z.{.... .....{.... .....+..*...}..... ....}..... ....}.....(.....*N.....~....

C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment Advice 80642111.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:xn:x
MD5:	F4E3CE3E7B581FF32E40968298BA013D
SHA1:	69E771474BA5705EB63F0E6A4FA885755279549E
SHA-256:	5B328CF43D53A589FE546B2D4E2D18E962693C58A78FD1E0AA6EB05501DBD81F
SHA-512:	30260997A27DDCBD88B5EA5F72FDA94E10A4FD883C8E11B274E940A3065E2FA997B7A4C28BE3A41B665841B987459B61FC2370EFB5243DFA76AC9B729916267A
Malicious:	false
Preview:	6228

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.359935487883289
Encrypted:	false
SSDEEP:	3:oNUkh4EaKC59KuCa:oN9aZ5v
MD5:	12D2EDA11A3448999A0FE3B16E86A9DC
SHA1:	BA191B82B2B86F0DCE06844378C6E9FEC1228C6F
SHA-256:	43F3713FB66C95CA2EF5D61548FC11BB1BFC86F9BC32F4BD3DB65B9A827F395B
SHA-512:	56EACBC7996ECD60F0688732D8084BB1B2EE7F74CC796A1AC97EA08FE97FA227FAC7DC7EB17F0CF3E0DE31D10C3BF35FC19F002AECC78F22267B5F0058519C44
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe

C:\Users\user\AppData\Roaming\pidloc.txt

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.991542962307303
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Payment Advice 80642111.exe
File size:	744448
MD5:	85bd30d4211b1dff2fe6847502341831
SHA1:	74fdf25bef9f31e311b21d8ca572f834d03134c0
SHA256:	6f2af9503a84bf2c99e0bbf735b953a7551f7ff78f87c9ad84e8aff091f2ae10
SHA512:	ebb2db3bf9315bfd4b307e587da544471512e56cc6b3414e6bcd4f48e65c1d27c3aebd16ac016794e9a540d11a7b1adbb233b4d4c0267e901fd0baac9341fc4e
SSDEEP:	12288:xR/SQVieUU3JGNECPXYjy7cBwUpyRsMd1B4w4wpHr+26W5mc5ubo7qkdUmTAZnrh:xR/SQVi7U3JGNfPIjLqUp7Md7ZHpR53r
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!(b.....0..R.....p.. .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b70de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xA4622821 [Thu May 24 02:17:05 2057 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb708c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x5d6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb50e4	0xb5200	False	0.943829796411	data	7.9941732776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x5d6	0x600	False	0.418619791667	data	4.12696293065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb80a0	0x34c	data		
RT_MANIFEST	0xb83ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

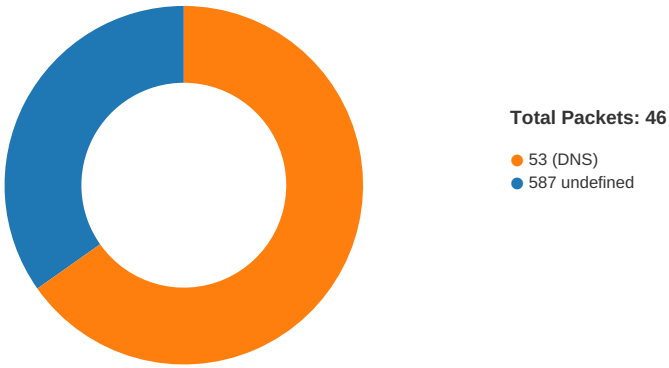
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	ScreenCapturer.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ScreenCapturer
ProductVersion	1.0.0.0
FileDescription	ScreenCapturer
OriginalFilename	ScreenCapturer.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:28:05.155992031 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:05.244574070 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:05.244694948 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:05.692012072 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:05.695194960 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:05.783704996 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:05.783732891 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:05.784580946 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:05.873239040 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:05.918263912 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:05.977410078 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.069293022 CET	587	49726	31.209.137.12	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:28:06.069333076 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:06.069355011 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:06.069454908 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.078835964 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.166965008 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:06.215189934 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.229089022 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.317192078 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:06.318304062 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.406965017 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:06.408186913 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:06.538579941 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:08.504204035 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:08.504808903 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:08.592305899 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:08.593302011 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:08.596236944 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:08.686605930 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:08.716736078 CET	49726	587	192.168.2.5	31.209.137.12
Feb 24, 2021 07:28:08.805481911 CET	587	49726	31.209.137.12	192.168.2.5
Feb 24, 2021 07:28:08.805589914 CET	49726	587	192.168.2.5	31.209.137.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:26:53.098968029 CET	52704	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:53.149944067 CET	52212	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:53.159224033 CET	53	52704	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:53.201551914 CET	53	52212	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:53.776766062 CET	54302	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:53.825568914 CET	53	54302	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:53.974134922 CET	53784	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:54.033963919 CET	53	53784	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:54.239633083 CET	65307	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:54.293395996 CET	53	65307	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:54.350033045 CET	64344	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:54.399267912 CET	53	64344	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:54.809977055 CET	62060	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:54.859361887 CET	53	62060	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:55.995503902 CET	61805	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:56.044677973 CET	53	61805	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:57.045861006 CET	54795	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:57.104499102 CET	53	54795	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:57.207887888 CET	49557	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:57.257030010 CET	53	49557	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:58.520972013 CET	61733	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:58.571281910 CET	53	61733	8.8.8.8	192.168.2.5
Feb 24, 2021 07:26:59.516694069 CET	65447	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:26:59.576988935 CET	53	65447	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:00.802773952 CET	52441	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:00.851752043 CET	53	52441	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:01.999958992 CET	62176	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:02.048999071 CET	53	62176	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:03.588164091 CET	59596	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:03.640224934 CET	53	59596	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:05.481010914 CET	65296	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:05.532744884 CET	53	65296	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:06.920413017 CET	63183	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:06.969310999 CET	53	63183	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:08.115135908 CET	60151	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:08.166940928 CET	53	60151	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:16.313922882 CET	56969	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:16.374413013 CET	53	56969	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:23.339302063 CET	55161	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 07:27:23.401890039 CET	53	55161	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:40.123382092 CET	54757	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:40.176876068 CET	53	54757	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:43.666390896 CET	49992	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:43.724270105 CET	53	49992	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:44.313889027 CET	60075	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:44.365324974 CET	53	60075	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:46.629843950 CET	55016	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:46.678950071 CET	53	55016	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:49.008070946 CET	64345	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:49.068207026 CET	53	64345	8.8.8.8	192.168.2.5
Feb 24, 2021 07:27:49.250905991 CET	57128	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:27:49.299901962 CET	53	57128	8.8.8.8	192.168.2.5
Feb 24, 2021 07:28:05.034975052 CET	54791	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:28:05.099201918 CET	53	54791	8.8.8.8	192.168.2.5
Feb 24, 2021 07:28:09.248765945 CET	50463	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:28:09.313528061 CET	53	50463	8.8.8.8	192.168.2.5
Feb 24, 2021 07:29:01.234761000 CET	50394	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:29:01.283891916 CET	53	50394	8.8.8.8	192.168.2.5
Feb 24, 2021 07:29:01.734401941 CET	58530	53	192.168.2.5	8.8.8.8
Feb 24, 2021 07:29:01.806427002 CET	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 07:27:16.313922882 CET	192.168.2.5	8.8.8.8	0xbe82	Standard query (0)	10.76.9.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 24, 2021 07:27:43.666390896 CET	192.168.2.5	8.8.8.8	0xdc7b	Standard query (0)	10.76.9.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 24, 2021 07:28:05.034975052 CET	192.168.2.5	8.8.8.8	0x9d34	Standard query (0)	smtp.vivaldi.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 07:27:16.374413013 CET	8.8.8.8	192.168.2.5	0xbe82	Name error (3)	10.76.9.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 24, 2021 07:27:43.724270105 CET	8.8.8.8	192.168.2.5	0xdc7b	Name error (3)	10.76.9.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 24, 2021 07:28:05.099201918 CET	8.8.8.8	192.168.2.5	0x9d34	No error (0)	smtp.vivaldi.net		31.209.137.12	A (IP address)	IN (0x0001)

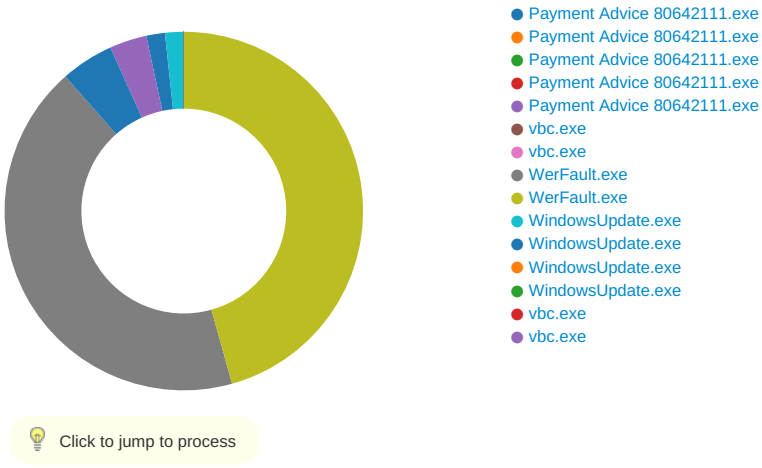
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 24, 2021 07:28:05.692012072 CET	587	49726	31.209.137.12	192.168.2.5	220 smtp.vivaldi.net ESMTP Postfix (Ubuntu)
Feb 24, 2021 07:28:05.695194960 CET	49726	587	192.168.2.5	31.209.137.12	EHLO 609290
Feb 24, 2021 07:28:05.783732891 CET	587	49726	31.209.137.12	192.168.2.5	250-smtp.vivaldi.net 250-PIPELINING 250-SIZE 36700160 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 SMTPUTF8
Feb 24, 2021 07:28:05.784580946 CET	49726	587	192.168.2.5	31.209.137.12	STARTTLS
Feb 24, 2021 07:28:05.873239040 CET	587	49726	31.209.137.12	192.168.2.5	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Payment Advice 80642111.exe PID: 6428 Parent PID: 5748

General

Start time:	07:27:01
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Advice 80642111.exe'
Imagebase:	0x6d0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.232301416.00000000039D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.232301416.00000000039D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.232301416.00000000039D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.232301416.00000000039D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.232301416.00000000039D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.232301416.00000000039D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.235200966.00000000050F0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Advice 80642111.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDBC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Advice 80642111.exe.log	unknown	706	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, C	success or wait	1	6DDBC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA85705	unknown

Analysis Process: Payment Advice 80642111.exe PID: 6464 Parent PID: 6428

General

Start time:	07:27:03
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Imagebase:	0x1d0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Payment Advice 80642111.exe PID: 6488 Parent PID: 6428

General

Start time:	07:27:03
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Imagebase:	0x2b0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Payment Advice 80642111.exe PID: 6496 Parent PID: 6428

General

Start time:	07:27:04
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Imagebase:	0x1d0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Payment Advice 80642111.exe PID: 6508 Parent PID: 6428

General

Start time:	07:27:04
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Payment Advice 80642111.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment Advice 80642111.exe

Imagebase:	0x5c0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.283540022.00000000039A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000004.00000002.293943590.0000000008500000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.278382516.0000000002931000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.278382516.0000000002931000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000004.00000002.294011237.0000000008650000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.283236826.0000000003939000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.275693727.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.275693727.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.275693727.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.275693727.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.275693727.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C8FDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WindowsUpdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C8FDD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 35 30 38	6508	success or wait	1	6C8F1B4F	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	51	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 50 61 79 6d 65 6e 74 20 41 64 76 69 63 65 20 38 30 36 34 32 31 31 31 2e 65 78 65	C:\Users\user\Desktop\Payment Advice 80642111.exe	success or wait	1	6C8F1B4F	WriteFile
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 21 28 62 a4 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 52 0b 00 00 08 00 00 00 00 00 00 de 70 0b 00 00 20 00 00 00 80 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......PE..L...!(b...............0..R...........p... ....@.. ....@.................	success or wait	3	6C8FDD66	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C8FDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA85705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8F1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Windows Update	unicode	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	6C8F646A	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	6C8FC075	RegSetValueExW

Analysis Process: vbc.exe PID: 7116 Parent PID: 6508

General

Start time:	07:27:23
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 7124 Parent PID: 6508

General

Start time:	07:27:23
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 3220 Parent PID: 7116

General

Start time:	07:27:25
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7116 -s 176
Imagebase:	0xcd0000
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	6FE01717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD7.tmp	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD7.tmp.xml	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF013.tmp.csv	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF525.tmp.txt	success or wait	1	6FDF4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 61 70 36 60 a4 05 12 00 00 00 00 00	MDMP........ ....ap6`........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.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 74 0b 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 cc 1b 00 00 5b 70 36 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 32 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 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......t..... ..GenuineIntelW...........T... ....[p6`.................. ....0..2............... 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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.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 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 a2 48 47 00 a2 48 47 00 00 90 25 00 a2 48 47 00 a2 48 47 00 27 8c 45 e8 94 ff 19 00 a4 48 47 00 23 00 00 00 46 02 01 00 84 ff 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+....HG..HG...%..HG..HG. '.E......HG.#...F.......+.........	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	168	d0 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 a4 48 47 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 b7 b8 b0 d0 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 e6 0b 00 00	........................HG...	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	20	05 00 00 00 00 90 25 00 00 00 00 00 98 04 00 00 d2 11 00 00	......%............	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	1176	00 00 00 00 ff ff ff ff 00 00 40 00 a0 7b ad 77 48 17 74 00 00 00 00 00 00 00 74 00 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 f8 7b ad 77 01 00 01 00 00 00 00 00 00 00 eb 7f 00 00 00 00 30 07 eb 7f 00 00 fb 7f 28 02 fc 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........@..{.wH.t.......t..y .w................................ {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	4	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	4220	bc 9a a2 77 a3 1a 32 77 aa aa aa aa b8 f1 19 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 ac 00 00 00 a8 00 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 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 aa 00 90 25 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 f1 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..2w..................... ....$........... .... %.............................	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 18 f1 19 00 bc 9a a2 77 23 00 00 00 06 02 00 00 88 ef 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... ....w#...........+.........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	48	d0 1b 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 c0 25 00 00 00 00 00 84 ef 19 00 00 00 00 00 7c 10 00 00 6a 28 00 00 cc 02 00 00 b2 0e 00 00	....%........... ..|...j(..........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	20	0e 00 00 00 76 00 62 00 63 00 2e 00 65 00 78 00 65 00 00 00	....v.b.c...e.x.e...	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	752	00 00 22 77 00 00 00 00 00 30 1e 00 ba e9 1e 00 fd b0 9a 14 c4 0b 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 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 50 55 02 00 00 00 00 00 a0 b7 02 00 00 00 00 85 4b 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 d2 dc 00 00 00 00 00 00 8e 4d 03 00 00 00 00 00 fd 90 02 00 00 00 00 00 57 18 08 00 00 00 00 00 e9 e6 17 00 00 00 00 00 40 ff 1f 00 00 00 00 00 94 f7 17 00 00 00 00	..“w.....0..... .....B.....B?..... .....(..... ..@A.....Zb..... ....PU..... .K.....M .....W..... @.....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	3196	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....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...(...W. a.i.t.C.o.m.p.l	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CA.tmp.dmp	unknown	108	03 00 00 00 34 00 00 00 fc 06 00 00 04 00 00 00 b4 01 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 7e 11 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 68 07 00 00 fa 3d 00 00 15 00 00 00 ec 01 00 00 f0 08 00 00 16 00 00 00 98 00 00 00 dc 0a 00 00	....4.....<.....T. ..~.....T.....8..... ....T.....h....=.....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.1.6.<./.P.i.d.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 62 00 63 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.>.v.b.c...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 30 00 30 00 30 00 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.2.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 36 00 30 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.>.6.6.0.3.<./.U.p.t.i.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 31 00 32 00 33 00 36 00 35 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.3.6.5.8.2.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 31 00 32 00 33 00 35 00 37 00 36 00 33 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.3.5.7.6.3.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.6.4.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 34 00 31 00 32 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.4.1.2.5.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 34 00 31 00 32 00 35 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.4.1.2.5.4.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.3.0.7.2.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 39 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.2.9.0.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.7.4.0.8.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.3.6.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.7.3.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.1.6.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.7.3.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.5.0.8.<./.P.i.d.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 61 00 79 00 6d 00 65 00 6e 00 74 00 20 00 41 00 64 00 76 00 69 00 63 00 65 00 20 00 38 00 30 00 36 00 34 00 32 00 31 00 31 00 31 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.>.P.a.y.m.e.n.t. .A.d.v.i.c.e. .8.0.6.4.2.1.1.1...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 35 00 33 00 31 00 32 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.>.2.5.3.1.2. <./.U.p.t.i.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 35 00 39 00 33 00 38 00 37 00 33 00 39 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.>.2.5.9.3.8.7.3.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 39 00 34 00 39 00 30 00 36 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.2.9.4.9.0.6.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 36 00 33 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.3.7.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 30 00 38 00 35 00 37 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.0.8.5.7.6.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 30 00 38 00 35 00 33 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.0.8.5.3.5.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 34 00 32 00 33 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.2.3.0.8.8.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 33 00 32 00 38 00 39 00 31 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.>.3.2.8.9.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 35 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.3.5.4.4.0.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.5.4.4.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 34 00 39 00 31 00 31 00 38 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.9.1.1.8.7.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 35 00 32 00 32 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.5.2.2.3.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 34 00 39 00 31 00 31 00 38 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.4.9.1.1.8.7.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	64	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 76 00 62 00 63 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.>.v.b.c...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 62 00 61 00 6a 00 6b 00 64 00 68 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.>.b.a.j.k.d.h.,. .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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 62 00 61 00 6a 00 6b 00 64 00 68 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.>.b.a.j.k.d.h.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 39 00 37 00 38 00 36 00 31 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.2.9.7.8.6.1.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 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.<./.F.l.a.g.s.>.	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 2d 00 32 00 34 00 54 00 31 00 35 00 3a 00 32 00 37 00 3a 00 33 00 30 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.-.0.2.-.2.4.T.1.5.:.2.7.:.3.0.Z.".>.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 31 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 37 00 31 00 38 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 37 00 31 00 38 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.=.".3.4.4.". .P.I.D.=.".7.1.1.6.". .U.p.t.i.m.e.M.S.=.".7.1.8.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.1.8.". .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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 30 00 63 00 38 00 31 00 65 00 34 00 37 00 2d 00 35 00 65 00 31 00 62 00 2d 00 34 00 39 00 33 00 34 00 2d 00 38 00 63 00 63 00 35 00 2d 00 38 00 63 00 33 00 63 00 31 00 62 00 31 00 64 00 34 00 39 00 37 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.3.0.c.8.1.e.4.7.-.5.e.1.b.-.4.9.3.4.-.8.c.c.5.-.8.c.3.c.1.b.1.d.4.9.7.5.<./.G.u.i.d.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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 32 00 2d 00 32 00 34 00 54 00 31 00 35 00 3a 00 32 00 37 00 3a 00 33 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.4.T.1.5.:.2.7.:.3.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5B.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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD7.tmp.xml	unknown	4643	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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada\Report.wer	unknown	2	ff fe	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada\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	135	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f0f7e6794544275e818a7614df8b65417782bd48_966227d3_0cdc2ada\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 36 00 39 00 31 00 32 00 39 00 30 00 34 00 30 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.6.9.1.2.9.0.4.0.3.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6FE11FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 A4 48 47 00 02 00 00 00 01 00 00 00 B7 B8 B0 D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6FE11FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: 204 Parent PID: 7124

General

Start time:	07:27:26
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7124 -s 176
Imagebase:	0xcd0000
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	6FE01717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f089e1f5158893287601d79f3806df6ebd7720_6c16ead4_0084324c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f089e1f5158893287601d79f3806df6ebd7720_6c16ead4_0084324c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDF497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp.xml	success or wait	1	6FDF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp.csv	success or wait	1	6FDF4BEF	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB61.tmp.txt	success or wait	1	6FDF4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 62 70 36 60 a4 05 12 00 00 00 00 00	MDMP..... .....bp6`.....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.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 74 0b 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 d4 1b 00 00 5b 70 36 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 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 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... .....[p6`..... .....0..2..... 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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.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 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 a2 48 47 00 a2 48 47 00 00 f0 22 00 a2 48 47 00 a2 48 47 00 e4 6b 10 ba 94 ff 19 00 a2 48 47 00 23 00 00 00 46 02 01 00 84 ff 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+....HG..HG..."..HG..HG.. k.......HG.#...F.......+.........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	168	d8 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 a2 48 47 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 e4 6b 10 ba ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 e6 0b 00 00	........................HG... ....k..........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	20	05 00 00 00 00 f0 22 00 00 00 00 00 98 04 00 00 d2 11 00 00	......"............	success or wait	5	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	1176	00 00 00 00 ff ff ff ff 00 00 40 00 a0 7b ad 77 48 17 56 00 00 00 00 00 00 00 56 00 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 f8 7b ad 77 01 00 01 00 00 00 00 00 00 00 eb 7f 00 00 00 00 30 07 eb 7f 00 00 fb 7f 28 02 fc 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........@..{.wH.V.......V..y .w................................ {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	4220	bc 9a a2 77 a3 1a 32 77 aa aa aa aa b8 f1 19 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 ac 00 00 00 a8 00 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 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 aa 00 f0 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 f1 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..2w...................... ....$........... .... ".............................	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 18 f1 19 00 bc 9a a2 77 23 00 00 00 06 02 00 00 88 ef 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#...........+.........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	48	d8 1b 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 20 23 00 00 00 00 00 84 ef 19 00 00 00 00 00 7c 10 00 00 6a 28 00 00 cc 02 00 00 b2 0e 00 00	.... #........... ..|...j(..........	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	20	0e 00 00 00 76 00 62 00 63 00 2e 00 65 00 78 00 65 00 00 00	....v.b.c...e.x.e...	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	752	00 00 22 77 00 00 00 00 00 30 1e 00 ba e9 1e 00 fd b0 9a 14 c4 0b 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 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 d0 45 02 00 00 00 00 00 a0 b7 02 00 00 00 00 02 4c 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 e6 e4 00 00 00 00 00 00 8e 4d 03 00 00 00 00 00 fd 90 02 00 00 00 00 00 b8 0c 08 00 00 00 00 00 88 f2 17 00 00 00 00 00 40 ff 1f 00 00 00 00 00 94 f7 17 00 00 00 00	.."w.....0.................... ....B.......B?........... ....(............. ..@A..................Zb...... ....E............ .L...........................M .... @.............	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	3196	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....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...(...W.a.i.t.C.o.m.p.l	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.dmp	unknown	108	03 00 00 00 34 00 00 00 fc 06 00 00 04 00 00 00 b4 01 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 7e 11 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 68 07 00 00 fa 3d 00 00 15 00 00 00 ec 01 00 00 f0 08 00 00 16 00 00 00 98 00 00 00 dc 0a 00 00	....4.....<.....T...~.....T.....8.....T.....h....=.....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.2.4.<./.P.i.d.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 62 00 63 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.>.v.b.c ...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 30 00 30 00 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u .r.e.>.0.0.0.0.0.0.0.2. <./.C.m. d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 35 00 35 00 35 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.>.7.5.5.5. <./.U.p.t.i.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 31 00 32 00 36 00 31 00 35 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.1.5.6.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 31 00 32 00 36 00 30 00 37 00 34 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.0.7.4.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 34 00 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.>.6.4.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 34 00 31 00 32 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.4.1.2.5.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 34 00 31 00 32 00 35 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.4.1.2.5.4.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.3.0.7.2.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 39 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.2.9.0.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.7.3.7.6.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.0.4.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.8.1.9.2.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 33 00 31 00 34 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.8.3.1.4.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.8.1.9.2.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.5.0.8.<./.P.i.d.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	100	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 61 00 79 00 6d 00 65 00 6e 00 74 00 20 00 41 00 64 00 76 00 69 00 63 00 65 00 20 00 38 00 30 00 36 00 34 00 32 00 31 00 31 00 31 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.>.P.a.y.m.e.n.t. .A.d.v.i.c.e. .8.0.6.4.2.1.1.1...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 36 00 31 00 35 00 36 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.>.2.6.1.5.6.<./.U.p.t.i.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 35 00 39 00 33 00 38 00 37 00 33 00 39 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.>.2.5.9.3.8.7.3.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 39 00 34 00 39 00 30 00 36 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.2.9.4.9.0.6.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 37 00 30 00 39 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.9.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 37 00 39 00 30 00 33 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.>.4.3.7.9.0.3.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 37 00 39 00 30 00 33 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.3.7.9.0.3.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 34 00 32 00 33 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.2.3.0.8.8.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 33 00 32 00 38 00 39 00 31 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.>.3.2.8.9.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 35 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.3.5.4.4.0.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.5.4.4.<./.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 34 00 39 00 31 00 31 00 38 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.9.1.1.8.7.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 35 00 32 00 32 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.5.2.2.3.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 34 00 39 00 31 00 31 00 38 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.4.9.1.1.8.7.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	64	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 76 00 62 00 63 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.>.v.b.c...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 62 00 61 00 6a 00 6b 00 64 00 68 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.>.b.a.j.k.d.h.,. .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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 62 00 61 00 6a 00 6b 00 64 00 68 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.>.b.a.j.k.d.h.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 39 00 37 00 38 00 36 00 31 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.2.9.7.8.6.1.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 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.<./.F.l.a.g.s.>.	success or wait	3	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 2d 00 32 00 34 00 54 00 31 00 35 00 3a 00 32 00 37 00 3a 00 33 00 31 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.-.0.2.-.2.4.T.1.5.:.2.7.:.3.1.Z.".>.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 33 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 33 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.5.". .P.I.D.=.".7.1.2.4.". .U.p.t.i.m.e.M.S.=.".1.0.3.1. ". .T.i.m.e.S.i.n.c.e.C.r.e.a. t.i.o.n.M.S.=.".1.0.3.1.". .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.=."	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 62 00 33 00 34 00 35 00 33 00 61 00 39 00 2d 00 30 00 38 00 62 00 35 00 2d 00 34 00 61 00 33 00 62 00 2d 00 62 00 66 00 64 00 39 00 2d 00 65 00 38 00 62 00 65 00 36 00 63 00 61 00 36 00 32 00 34 00 65 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.b.3.4.5.3.a.9.-.0.8.b.5.-.4.a.3.b.-.b.f.d.9.-.e.8.b.e.6.c.a.6.2.4.e.7.<./.G.u.i.d.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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 32 00 2d 00 32 00 34 00 54 00 31 00 35 00 3a 00 32 00 37 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.4.T.1.5.:.2.7.:.3.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE5.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	6FDF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF67E.tmp.xml	unknown	4643	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	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f089e1f5158893287601d79f3806df6ebd7720_6c16ead4_0084324c\Report.wer	unknown	2	ff fe	..	success or wait	1	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f089e1f5158893287601d79f3806df6ebd7720_6c16ead4_0084324c\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	135	6FDF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_f089e1f5158893287601d79f3806df6ebd7720_6c16ead4_0084324c\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 36 00 33 00 33 00 32 00 37 00 35 00 37 00 39 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.6.3.3.2.7.5.7.9.5.	success or wait	1	6FDF497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FDF43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	FileId	unicode	0000787d9a6ec3f262e8b71d19ac157c2a286a0f59dd	success or wait	1	6FE136BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	LowerCaseLongPath	unicode	c:\windows\microsoft.net\framework\v2.0.50727\vbc.exe	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	LongPathHash	unicode	vbc.exe|9d6f9af	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Name	unicode	vbc.exe	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Publisher	unicode	microsoft corporation	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Version	unicode	8.0.50727.8922	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	BinFileVersion	unicode	8.0.50727.8922	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	BinaryType	unicode	pe32_i386	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	ProductName	unicode	microsoft. visual studio. 2005	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	ProductVersion	unicode	8.0.50727.8922	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	LinkDate	unicode	02/08/2018 07:12:15	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	BinProductVersion	unicode	8.0.50727.8922	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Size	B	88 E0 11 00 00 00 00 00	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Language	dword	1033	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	IsPeFile	dword	1	success or wait	1	6FE136BF	unknown
\REGISTRY\A\{6e92e4b2-589f-80ce-3588-1312e3662cd1}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	IsOsComponent	dword	1	success or wait	1	6FE136BF	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 A4 48 47 00 02 00 00 00 01 00 00 00 B7 B8 B0 D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 A2 48 47 00 02 00 00 00 01 00 00 00 E4 6B 10 BA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6FE11FE8	RegSetValueExW

Analysis Process: WindowsUpdate.exe PID: 5480 Parent PID: 3472

General

Start time:	07:27:30
Start date:	24/02/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0x350000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000015.00000002.309460071.0000000004DF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.303042650.00000000037F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, Metadefender, Browse • Detection: 68%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WindowsUpdate.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDBC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WindowsUpdate.exe.log	unknown	706	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, C	success or wait	1	6DDBC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA85705	unknown

Analysis Process: WindowsUpdate.exe PID: 6228 Parent PID: 5480

General

Start time:	07:27:33
Start date:	24/02/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Imagebase:	0x6e0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000017.00000002.507838378.0000000007CD0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000017.00000002.507820706.0000000007CC0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.495351637.0000000002D21000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000017.00000002.495351637.0000000002D21000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000017.00000002.503528098.0000000003D95000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000017.00000002.488882188.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000002.488882188.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000017.00000002.488882188.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000017.00000002.488882188.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000017.00000002.488882188.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000002.503465573.0000000003D21000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DAACF06	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C8F1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	success or wait	1	6C8F6A95	DeleteFileW
C:\Users\user\AppData\Roaming\pidloc.txt	success or wait	1	6C8F6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	6C8F6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	6C8F6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	36 32 32 38	6228	success or wait	1	6C8F1B4F	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	49	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 57 69 6e 64 6f 77 73 55 70 64 61 74 65 2e 65 78 65	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	6C8F1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	4096	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	6DA6D72F	unknown
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	6C8F1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	6C8F1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	6C8F1B4F	ReadFile

Analysis Process: WindowsUpdate.exe PID: 804 Parent PID: 3472

General

Start time:	07:27:38
Start date:	24/02/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0xaf0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000001A.00000002.327982502.0000000005620000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001A.00000002.318746225.0000000003FA9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: WindowsUpdate.exe PID: 6992 Parent PID: 804

General

Start time:	07:27:42
Start date:	24/02/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Imagebase:	0xfb0000
File size:	744448 bytes
MD5 hash:	85BD30D4211B1DFF2FE6847502341831
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001B.00000002.321590143.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000002.321590143.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001B.00000002.321590143.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001B.00000002.321590143.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001B.00000002.321590143.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: vbc.exe PID: 6452 Parent PID: 6228

General

Start time:	07:27:53
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.346347222.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 6876 Parent PID: 6228

General

Start time:	07:27:53
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.343283889.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis