ID: 362120
Sample Name: 5O857649056366403032021.PDF.exe
Cookbook: default.jbs
Time: 17:13:51
Date: 03/03/2021
Version: 31.0.0 Emerald

Table of Contents

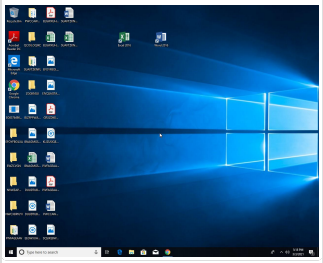
Analysis Report 5O85764905636640303202 1.PDF.exe

Overview

General Information

Sample Name:	5O85764905636640303202 1.PDF.exe
Analysis ID:	362120
MD5:	a67f05d542bcee4.
SHA1:	eeb590aaa3c478..
SHA256:	1e96629ba4b537..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

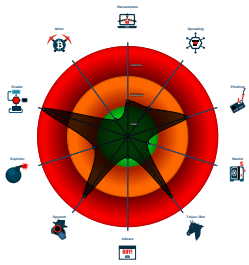
HawkEye
MailPassView

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 subm…
- Sigma detected: Suspicious Double …
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- 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**
- 5O857649056366403032021.PDF.exe (PID: 3468 cmdline: 'C:\Users\user\Desktop\5O857649056366403032021.PDF.exe' MD5: A67F05D542BCEE462ECC03AE4D8195D6)
  - 5O857649056366403032021.PDF.exe (PID: 5444 cmdline: C:\Users\user\Desktop\5O857649056366403032021.PDF.exe MD5: A67F05D542BCEE462ECC03AE4D8195D6)
    - vbc.exe (PID: 6732 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: 6844 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6732 -s 516 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - vbc.exe (PID: 6724 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.218552903.00000000027D1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.784876138.000000000872 0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000002.00000002.767924598.000000000040 2000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b719:$key: HawkEyeKeylogger • 0x7d917:$salt: 099u787978786 • 0x7bd32:$string1: HawkEye_Keylogger • 0x7cb85:$string1: HawkEye_Keylogger • 0x7d877:$string1: HawkEye_Keylogger • 0x7c11b:$string2: holdermail.txt • 0x7c13b:$string2: holdermail.txt • 0x7c05d:$string3: wallet.dat • 0x7c075:$string3: wallet.dat • 0x7c08b:$string3: wallet.dat • 0x7d459:$string4: Keylog Records • 0x7d771:$string4: Keylog Records • 0x7d96f:$string5: do not script --> • 0x7b701:$string6: \pidloc.txt • 0x7b767:$string7: BSPLIT • 0x7b777:$string7: BSPLIT
00000002.00000002.767924598.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000002.00000002.767924598.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
2.2.5O857649056366403032021.PDF.exe.8890 000.12.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
2.2.5O857649056366403032021.PDF.exe.8720 000.11.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
2.2.5O857649056366403032021.PDF.exe.41a9 930.7.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
2.2.5O857649056366403032021.PDF.exe.41a9 930.7.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 58 entries				

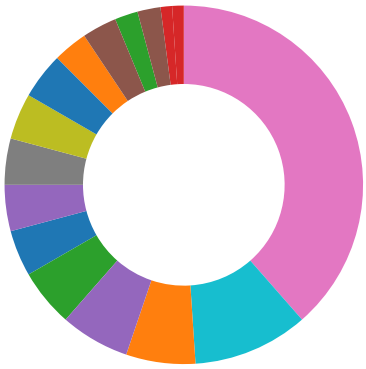
Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview

- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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 submitted 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

Hooking and other Techniques for Hiding and Protection:

- Changes the view of files in windows explorer (hidden files and folders)
- Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Opens the same file many times (likely Sandbox evasion)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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 steal Instant Messenger accounts or passwords
- Tries to steal Mail credentials (via file access)
- Tries to steal Mail credentials (via file registry)
- Yara detected WebBrowserPassView password recovery tool

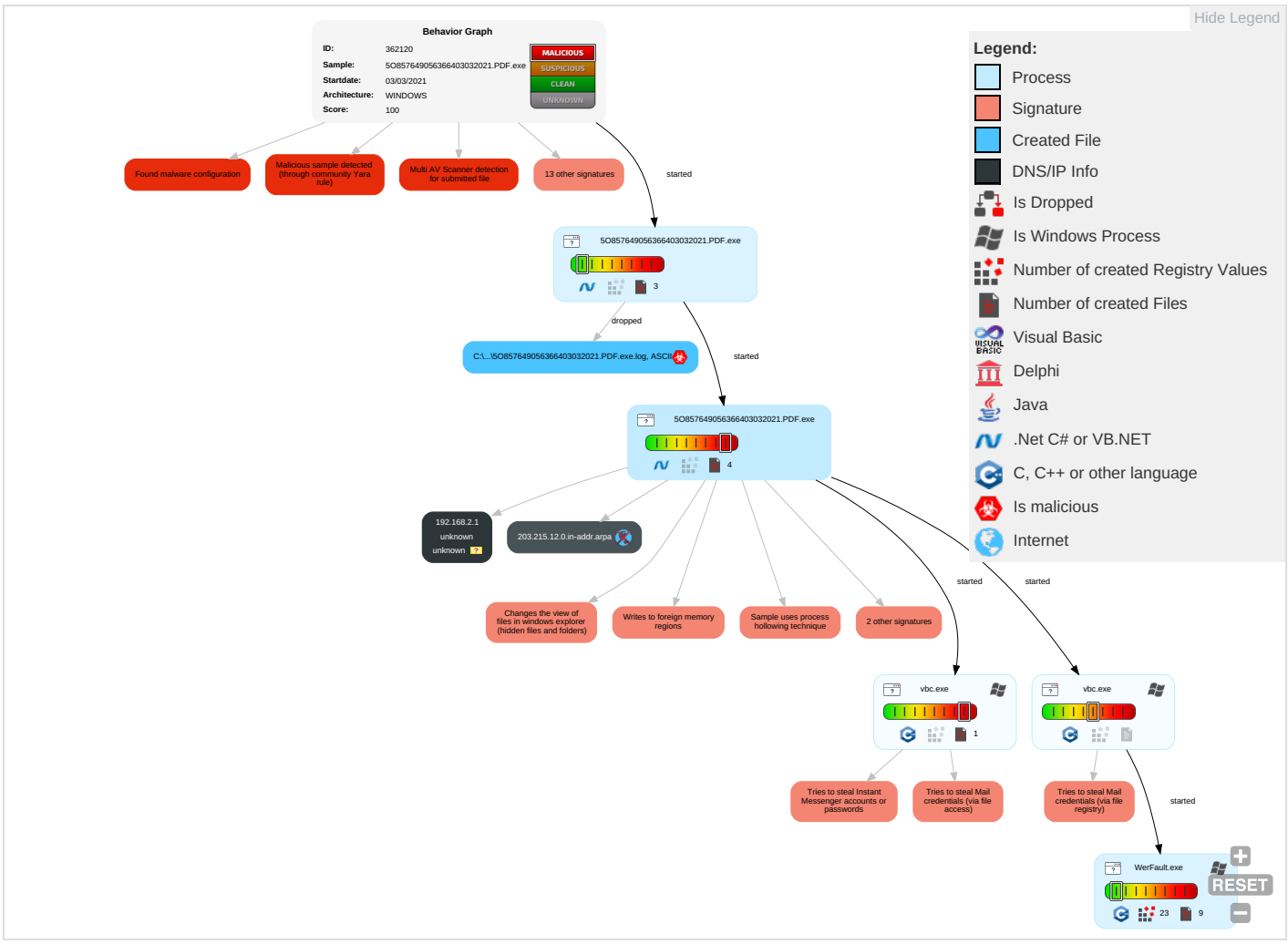
Remote Access Functionality:

- 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	Comm and C
Replication Through Removable Media 1	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 2	Peripheral Device Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Remot Softwa
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1 4 1	Credentials In Files 1	Account Discovery 1	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Applic Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	System Information Discovery 1 7	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	Virtualization/Sandbox Evasion 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

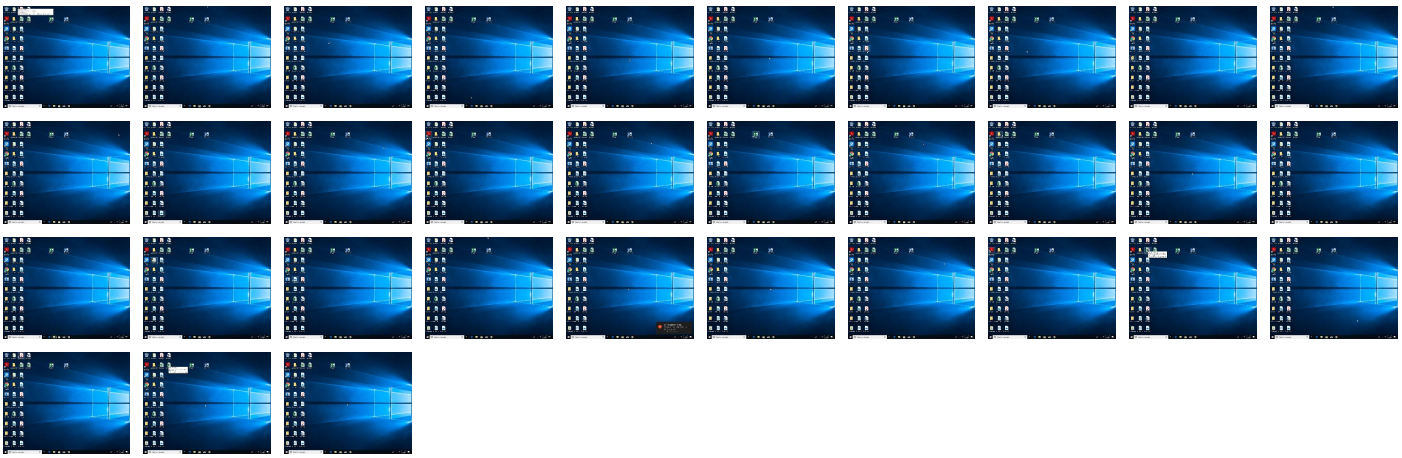
Behavior Graph



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
5O857649056366403032021.PDF.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	
5O857649056366403032021.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
2.2.5O857649056366403032021.PDF.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
2.2.5O857649056366403032021.PDF.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.5O857649056366403032021.PDF.exe.3c22610.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnO	0%	Avira URL Cloud	safe	
http://www.carterandcone.comadeh	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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com/	0%	Avira URL Cloud	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comceTF	0%	Avira URL Cloud	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.founder.com.cn/cnr-c	0%	Avira URL Cloud	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.monotype.t	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/X	0%	Avira URL Cloud	safe	
http://www.carterandcone.comht	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC1	0%	Avira URL Cloud	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.carterandcone.comTC/	0%	Avira URL Cloud	safe	
http://www.carterandcone.comitk	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krny	0%	Avira URL Cloud	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.carterandcone.comTC3	0%	Avira URL Cloud	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.galapagosdesign.com/staff/dennis.htmR	0%	Avira URL Cloud	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://www.carterandcone.commpa	0%	Avira URL Cloud	safe	
http://www.carterandcone.comb	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.comf	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsof	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.sandoll.co.krn	0%	Avira URL Cloud	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.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.sakkal.com8	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comn	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krF	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://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://www.carterandcone.comghtv	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.-	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.agfamonotype.0	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krn-u	0%	Avira URL Cloud	safe	
http://www.carterandcone.comark	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn&	0%	Avira URL Cloud	safe	
http://www.carterandcone.comies	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
203.215.12.0.in-addr.arpa	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnO	5O85764905636640303202 1.PDF.exe, 00000002.00000003.222841537.000000000626E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comadeh	5O85764905636640303202 1.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

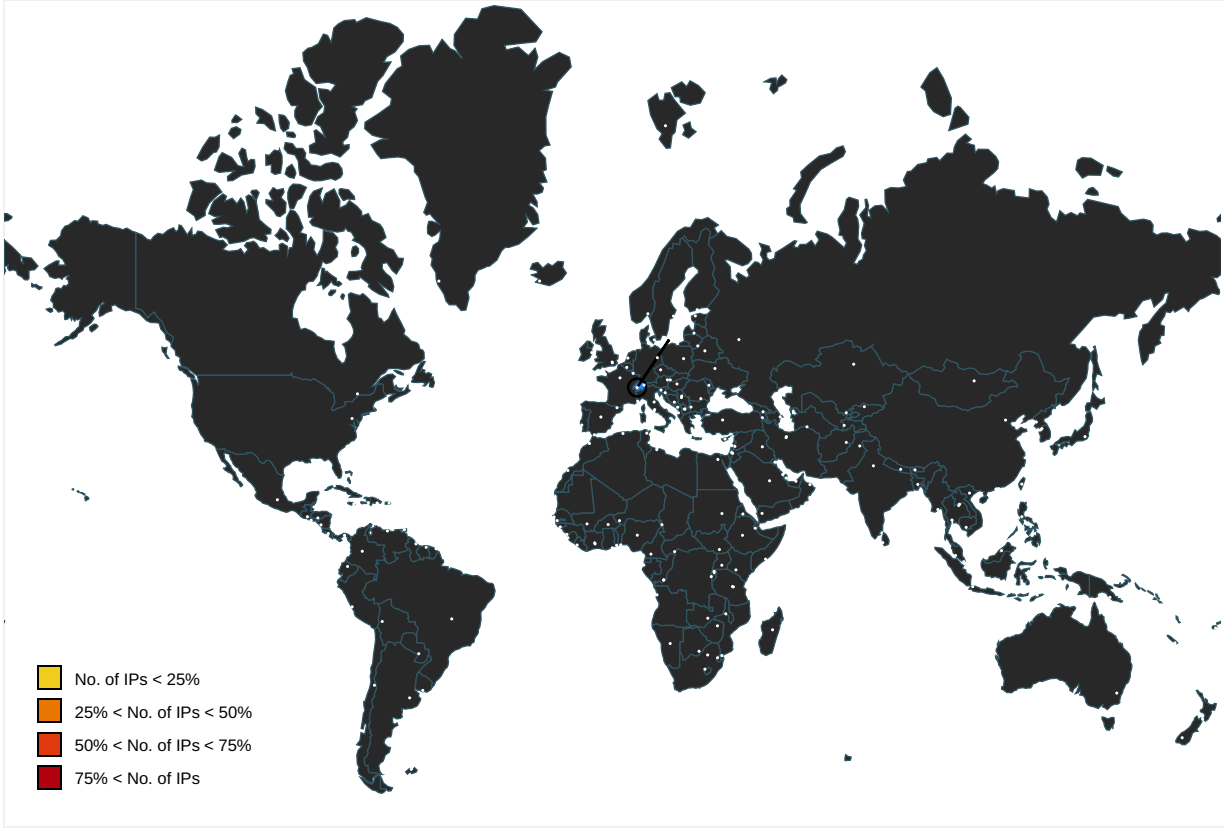
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersW	5O85764905636640303 2021.PDF.exe, 00000002.00000003.232516116.0000000006268000.00000004.00000001.sdmp	false		high
http://www.tiro.com	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com/	5O85764905636640303 2021.PDF.exe, 00000002.00000003.223882735.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp, 5O85764905636640303 2021.PDF.exe, 00000002.00000003.243602370.0000000006268000.00000004.00000001.sdmp, 5O85764905636640303 2021.PDF.exe, 00000002.00000003.243672472.0000000006268000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/O	5O85764905636640303 2021.PDF.exe, 00000002.00000003.229591196.0000000006278000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp, 5O85764905636640303 2021.PDF.exe, 00000002.00000003.222340087.000000000626E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	5O85764905636640303 2021.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp, 5O85764905636640303 2021.PDF.exe, 00000002.00000003.224185573.0000000006268000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comceTF	5O85764905636640303 2021.PDF.exe, 00000002.00000002.772908055.00000000014F7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	5O85764905636640303 2021.PDF.exe, 00000000.00000002.218552903.00000000027D1000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnr-c	5O85764905636640303 2021.PDF.exe, 00000002.00000003.223199362.0000000006265000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	5O85764905636640303 2021.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.t	5O85764905636640303 2021.PDF.exe, 00000002.00000003.240555318.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/X	5O85764905636640303202 1.PDF.exe, 00000002.00000003.223388192.0000000006265000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comht	5O85764905636640303202 1.PDF.exe, 00000002.00000003.224554700.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/-	5O85764905636640303202 1.PDF.exe, 00000000.00000002.219158430.00000000037D9000.00000004.00000001.sdmp, 5O8576490563664030 32021.PDF.exe, 00000002.00000002.767924598.0000000000402000.00000040.00000001.sdmp	false		high
http://www.carterandcone.comTC1	5O85764905636640303202 1.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC/	5O85764905636640303202 1.PDF.exe, 00000002.00000003.224185573.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comitk	5O85764905636640303202 1.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.yahoo.com/config/login	vbc.exe	false		high
http://www.fonts.com	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.krny	5O85764905636640303202 1.PDF.exe, 00000002.00000003.222340087.000000000626E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	5O85764905636640303202 1.PDF.exe, 00000002.00000003.222273989.000000000626E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	5O85764905636640303202 1.PDF.exe, 00000002.00000002.774686882.00000000031A1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTC3	5O85764905636640303202 1.PDF.exe, 00000002.00000003.224554700.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	vbc.exe, vbc.exe, 00000008.00000002.262898420.0000000000400000.00000040.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	5O85764905636640303202 1.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmR	5O85764905636640303202 1.PDF.exe, 00000002.00000003.236539415.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	5O85764905636640303202 1.PDF.exe, 00000000.00000002.218552903.00000000027D1000.00000004.00000001.sdmp, 5O8576490563664030 32021.PDF.exe, 00000002.00000002.774686882.00000000031A1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	5O85764905636640303202 1.PDF.exe, 00000002.00000003.227490771.0000000006268000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.commpa	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerst	5O8576490563664030320 21.PDF.exe, 00000002.00000003.233214847.0000000006268000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersr	5O8576490563664030320 21.PDF.exe, 00000002.00000003.232557212.0000000006268000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comb	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224554700.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	5O8576490563664030320 21.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	5O8576490563664030320 21.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	5O8576490563664030320 21.PDF.exe, 00000002.00000003.235768370.0000000006278000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comf	5O8576490563664030320 21.PDF.exe, 00000002.00000003.227770906.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comsof	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krn	5O8576490563664030320 21.PDF.exe, 00000002.00000003.222652479.000000000626E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	5O8576490563664030320 21.PDF.exe, 00000002.00000002.772908055.00000000014F7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.come.com	5O8576490563664030320 21.PDF.exe, 00000002.00000002.772908055.00000000014F7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com8	5O8576490563664030320 21.PDF.exe, 00000002.00000003.227490771.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224554700.0000000006268000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comn	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krF	5O8576490563664030320 21.PDF.exe, 00000002.00000003.222340087.000000000626E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	5O8576490563664030320 21.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	5O8576490563664030320 21.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	5O8576490563664030320 21.PDF.exe, 00000002.00000003.222841537.000000000626E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	5O8576490563664030321.PDF.exe, 00000002.00000003.231534012.0000000006268000.00000004.00000001.sdmp, 5O8576490563664030321.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comghtv	5O8576490563664030321.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	5O8576490563664030321.PDF.exe, 00000002.00000003.238156321.0000000006268000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.-	5O8576490563664030321.PDF.exe, 00000002.00000003.234952955.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.galapagosdesign.com/9	5O8576490563664030321.PDF.exe, 00000002.00000003.235768370.0000000006278000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	5O8576490563664030321.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	5O8576490563664030321.PDF.exe, 00000002.00000002.782376344.0000000007452000.00000004.00000001.sdmp	false		high
http://www.agfamonotype.0	5O8576490563664030321.PDF.exe, 00000002.00000003.243737730.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sandoll.co.krn-u	5O8576490563664030321.PDF.exe, 00000002.00000003.222340087.000000000626E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers:	5O8576490563664030321.PDF.exe, 00000002.00000003.231609808.0000000006268000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comark	5O8576490563664030321.PDF.exe, 00000002.00000003.224323142.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn&	5O8576490563664030321.PDF.exe, 00000002.00000003.223199362.0000000006265000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	5O8576490563664030321.PDF.exe, 00000002.00000003.229567284.0000000006268000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comies	5O8576490563664030321.PDF.exe, 00000002.00000003.224083852.0000000006268000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	362120
Start date:	03.03.2021
Start time:	17:13:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5O857649056366403032021.PDF.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:	35
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@8/7@1/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 4.1% (good quality ratio 3.9%) • Quality average: 85.1% • Quality standard deviation: 23.6%
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, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 131.253.33.200, 13.107.22.200, 51.11.168.160, 184.30.21.219, 104.43.193.48, 40.88.32.150, 23.211.6.115, 104.42.151.234, 52.255.188.83, 184.30.20.56, 8.248.135.254, 8.241.122.254, 8.241.11.126, 8.241.123.254, 8.248.131.254, 2.20.142.209, 2.20.142.210, 51.104.139.180, 92.122.213.247, 92.122.213.194, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.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, storeedgefd.xbetservices.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, 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, storeedgefd.dsx.mp.microsoft.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.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, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Execution Graph export aborted for target vbc.exe, PID 6732 because there are no executed function • 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:14:43	API Interceptor	6x Sleep call for process: 5O857649056366403032021.PDF.exe modified
17:15:12	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_29b1fd91934ca85fd856bebf7e23b59544bb3f14_6c16ead4_1afe9588\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10936
Entropy (8bit):	3.773645507675144
Encrypted:	false
SSDEEP:	192:+oRmKDX5HBUZMXQf9jU3//u7swS274ItE7GDBh:NbDZBUZMXojM/u7swX4ItEOn
MD5:	B990CB6AF75858E6F2C29C7A53953022
SHA1:	43D20E7FF25881476A44DBA8066C662B9D6F9D65
SHA-256:	840F9558BFC0DF3028B17747557F6164B8E047E9731644A87B3141550915A256
SHA-512:	B71B19F6D1A887457695FDBF710EC4A5ED4592B19D9573FBA4F01DF34C7704113E762817D7E0284146318D75CB699EA51A259192A717D09A17956343104F77E3
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.=.1.3.2.5.9.2.9.4.1.0.9.1.1.4.0.7.2.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.9.2.9.4.1.1.0.3.1.7.1.9.7.6.....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.=.5.d.d.e.a.9.d.1.-.6.f.0.4.-.4.2.8.b.-.9.b.7.2.-.7.d.1.1.7.3.0.7.d.6.d.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.e.7.4.c.3.7.e.-.b.e.f.5.-.4.5.b.1.-.8.d.0.c.-.7.a.f.0.5.a.f.f.2.7.3.1.....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.a.4.c.-.0.0.0.1.-.0.0.1.7.-.7.6.a.0.-.3.8.c.f.9.3.1.0.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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\WER89A1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	
File Type:	Mini DuMP crash report, 14 streams, Thu Mar 4 01:15:09 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	37050
Entropy (8bit):	2.0647926238959364
Encrypted:	false
SSDEEP:	192:mrNMAoQcWWXDPJk2Y+CVRd5AveQFkJQHN:mxLD1MDPJNYpVRYVFtN
MD5:	A2F4BCACEA6B487455496EC0281A8FE7
SHA1:	4AE0F67C760C25F5A15ADB46BC37FECC07E2B965
SHA-256:	29A4BB5E95C231AB869D21CC52C38715C301C284C929A6373ECA620166B6370F
SHA-512:	C801CDEE2BD1999FE06174664428CEB3C6C898F1D4782F3F6D327D5BA3497297CC4F079337CAD4B07D3D14FE8A462CDC8681F9A5C69508C391A1E8E3091CA4
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....4@`.....U.....B.....GenuineIntelW.....T.....L...4@`.....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\WER8BF4.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):	8344
Entropy (8bit):	3.703927038018695
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimG6A76Yqy6fFgmf5BSMCprY89bof7wsftv4m:RrlsNi36O6Yn69gmfPSRovfP
MD5:	9945E1B9A8D937B18F9DC31E975F1215
SHA1:	D61DCA56AAB3B6A1EE3B673D21BFA85086BDECAD
SHA-256:	0524E26D1CAA772616E33EBE260F28969494A6005A7ECECF6C563FCFCDBEB0EE
SHA-512:	62A8E6240F47C58371DF1B8E99872777F0C9B6832AAE413A9F7FEED95CF45E9BBC91D4934372DD7C587392E54A576D2FF5A49112D950B42889DBDA386BDE76C
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.>.6.7.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D8B.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):	4.480489970942812
Encrypted:	false
SSDEEP:	48:cvIwSD8zs8iJgtWI9q0WSC8Bg8fm8M4JlEZFqXK+q8VUwlMSHOd:uITfh9tSNTJauXKJwlTHOd
MD5:	9CCE89CAAB7F11B1DC13431E291B8398
SHA1:	365BDCF2293020750BFFB7F152B6834BE896D161
SHA-256:	DEF6B8F3897C80489FA0764A912542D8A4340DCB5ED74E6FB6115CC0C3550F1B
SHA-512:	1E2ED9E04CE0E1FA1900BE7C60346E40A1D089A02DC0E97DF8434657067F4185092A361EFE2FCDDD794CFCD028326A264217C1C92E6954EB115731B52951CFE
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="886225" />.. <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\5O8576490563664030 32021.PDF.exe.log	
Process:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5O857649056366403032021.PDF.exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	3:E3n:E3n
MD5:	587B7B833034299FDD5F4B10E7DC9FCA
SHA1:	4B9F94F92A6FFAEE7BF14533AE679C1D396EBBB7
SHA-256:	739B312AE914CFC44AB85100D93F3BA28C22DFE7FBBD4CEE9072C19A11D87411
SHA-512:	767B4ACB5EAA5C81E7810C3571818BA44BF35934991D46D80B3AAF4F33F73B313861D5AE58F0BFFBA2DE7FAD455D62923D4EDC5DC1AEAF30B12C652D7EC96223
Malicious:	false
Reputation:	low
Preview:	5444

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.712949307598833
Encrypted:	false
SSDEEP:	3:oNWXp5vQqhWfR88XukA:oNWXpFQSWxDA
MD5:	CCDB3AB1EE56552E9E8D0D47D18B1C78
SHA1:	8B56F93FB2AC5E73F461E8742C26062E9B82B22D
SHA-256:	A6884B2FA05A5C130256A76EC80C1B88F854A967A4B1DC966774A94DB0C0A4AB
SHA-512:	C6E1F1815014566DDF8AA8973431B85A713E94D7008A2B403F9A4995F72FA89C55EBBF740F1860F6E115219460621291A7255EE6D250592AD27A3CE8FC7C6C4D
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.637398703052732

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	5O857649056366403032021.PDF.exe
File size:	1057280
MD5:	a67f05d542bcee462ecc03ae4d8195d6
SHA1:	eeb590aaa3c47851ae6f678c29aec2ba1b54df8f
SHA256:	1e96629ba4b537932150cc517455a0cfddcb7c35a4a0998d107643dc887b31c3
SHA512:	270f31f9481dd1259a890de29b22c59adc21fbeaad17ff3c22ed739214d3ea490b086dd0ec8b92fa9f1e9d3cbda5e3ca97406d2d4f18e4a87ba09e0ac83deaa5
SSDEEP:	24576:c4ZIZrK3Orlv80WSRbvuvDzAolFCdNtlEBIQxBwqA:3Zd3xSRK4olkdQE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...x.>`.....P.....N7... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50374e
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:	0x603EE278 [Wed Mar 3 01:12:24 2021 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x103700	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x104000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x106000	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	0x101754	0x101800	False	0.826626972087	data	7.64304839327	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x104000	0x600	0x600	False	0.434244791667	data	4.20816553114	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x106000	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	0x104090	0x370	data		
RT_MANIFEST	0x104410	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 - 2021
Assembly Version	1.0.0.0
InternalName	NotSupportedException.exe
FileVersion	1.0.0.0
CompanyName	Agario
LegalTrademarks	
Comments	
ProductName	Snake Game
ProductVersion	1.0.0.0
FileDescription	Snake Game
OriginalFilename	NotSupportedException.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 3, 2021 17:14:33.214509964 CET	49873	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:33.260349989 CET	53	49873	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:33.709773064 CET	53196	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:33.758582115 CET	53	53196	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:33.914417982 CET	56777	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:33.960149050 CET	53	56777	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:34.240216017 CET	58643	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:34.321981907 CET	53	58643	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:34.408603907 CET	60985	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:34.456425905 CET	53	60985	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:35.405508041 CET	50200	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:35.451615095 CET	53	50200	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:36.435086966 CET	51281	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:36.491914988 CET	53	51281	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:37.438740969 CET	49199	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:37.483431101 CET	50620	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:37.484256983 CET	53	49199	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:37.543839931 CET	53	50620	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:39.445708990 CET	64938	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:39.491714954 CET	53	64938	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:40.667319059 CET	60152	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:40.716125965 CET	53	60152	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:41.989645958 CET	57544	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:42.037026882 CET	53	57544	8.8.8.8	192.168.2.3
Mar 3, 2021 17:14:58.696459055 CET	55984	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:14:58.753180027 CET	53	55984	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:01.106949091 CET	64185	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:01.152890921 CET	53	64185	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:01.163681030 CET	65110	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:01.214071035 CET	53	65110	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:02.767374039 CET	58361	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:02.813678980 CET	53	58361	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:04.194222927 CET	63492	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:04.240705967 CET	53	63492	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:05.250946045 CET	60831	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:05.299650908 CET	53	60831	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:06.904519081 CET	60100	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:06.950258017 CET	53	60100	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:08.590962887 CET	53195	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:08.636954069 CET	53	53195	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:09.509015083 CET	50141	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:09.568008900 CET	53	50141	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:10.655904055 CET	53023	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 3, 2021 17:15:10.701605082 CET	53	53023	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:11.877171993 CET	49563	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:11.922899961 CET	53	49563	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:12.121400118 CET	51352	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:12.171503067 CET	53	51352	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:13.808252096 CET	59349	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:13.857146978 CET	53	59349	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:14.778565884 CET	57084	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:14.824393034 CET	53	57084	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:20.228868008 CET	58823	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:20.274827003 CET	53	58823	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:29.668606043 CET	57568	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:29.716171026 CET	53	57568	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:29.807586908 CET	50540	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:29.863745928 CET	53	50540	8.8.8.8	192.168.2.3
Mar 3, 2021 17:15:48.932668924 CET	54366	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:15:48.981421947 CET	53	54366	8.8.8.8	192.168.2.3
Mar 3, 2021 17:16:01.827075958 CET	53034	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:16:01.872833967 CET	53	53034	8.8.8.8	192.168.2.3
Mar 3, 2021 17:16:20.140646935 CET	57762	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:16:20.196206093 CET	53	57762	8.8.8.8	192.168.2.3
Mar 3, 2021 17:16:53.634814978 CET	55435	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:16:53.682331085 CET	53	55435	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:12.506916046 CET	50713	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:12.556099892 CET	53	50713	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:30.583940029 CET	56132	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:30.643706083 CET	53	56132	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:32.108513117 CET	58987	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:32.167363882 CET	53	58987	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:32.696746111 CET	56579	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:32.742829084 CET	53	56579	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:33.303934097 CET	60633	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:33.375474930 CET	53	60633	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:34.003638983 CET	61292	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:34.068038940 CET	53	61292	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:38.208647966 CET	63619	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:38.269738913 CET	53	63619	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:38.780533075 CET	64938	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:38.835195065 CET	53	64938	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:39.593573093 CET	61946	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:39.642622948 CET	53	61946	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:40.453255892 CET	64910	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:40.512172937 CET	53	64910	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:41.080837965 CET	52123	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:41.153503895 CET	53	52123	8.8.8.8	192.168.2.3
Mar 3, 2021 17:17:54.798070908 CET	56130	53	192.168.2.3	8.8.8.8
Mar 3, 2021 17:17:54.860306978 CET	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 3, 2021 17:15:01.163681030 CET	192.168.2.3	8.8.8.8	0x589c	Standard query (0)	203.215.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

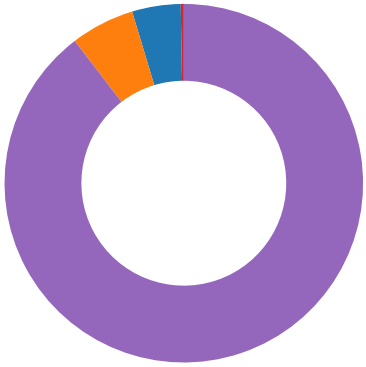
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 3, 2021 17:15:01.214071035 CET	8.8.8.8	192.168.2.3	0x589c	Name error (3)	203.215.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

Code Manipulations

Statistics

Behavior



5O857649056366403032021.PDF.e..
5O857649056366403032021.PDF.e..
vbc.exe
vbc.exe
WerFault.exe

Click to jump to process

System Behavior

Analysis Process: 5O857649056366403032021.PDF.exe PID: 3468 Parent PID: 5832

General

Start time:	17:14:41
Start date:	03/03/2021
Path:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5O857649056366403032021.PDF.exe'
Imagebase:	0x340000
File size:	1057280 bytes
MD5 hash:	A67F05D542BCEE462ECC03AE4D8195D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.218552903.00000000027D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.219158430.00000000037D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.219158430.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.219158430.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.219158430.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.219158430.00000000037D9000.00000004.00000001.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	6DE8CF06	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	6DE8CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5O857649056366403032021.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E19C78D	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\5O857649056366403032021.PDF.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 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 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E19C907	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	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile

Analysis Process: 5O857649056366403032021.PDF.exe PID: 5444 Parent PID: 3468

General

Start time:	17:14:44
Start date:	03/03/2021
Path:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe
Imagebase:	0xca0000
File size:	1057280 bytes
MD5 hash:	A67F05D542BCEE462ECC03AE4D8195D6
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: 00000002.00000002.784876138.0000000008720000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000002.00000002.767924598.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.767924598.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.767924598.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.767924598.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.767924598.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000002.00000002.778097540.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.778097540.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000002.00000002.785047145.0000000008890000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.774686882.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000002.00000002.774686882.00000000031A1000.00000004.00000001.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	6DE8CF06	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	6DE8CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CCD1E60	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	6CCD1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	6CCD6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	35 34 34 34	5444	success or wait	1	6CCD1B4F	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	54	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 35 4f 38 35 37 36 34 39 30 35 36 33 36 36 34 30 33 30 33 32 30 32 31 2e 50 44 46 2e 65 78 65	C:\Users\user\Desktop\5O857649056366403032021.PDF.exe	success or wait	1	6CCD1B4F	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	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	6CCD1B4F	ReadFile

Registry Activities

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	6CCDC075	RegSetValueExW

Analysis Process: vbc.exe PID: 6732 Parent PID: 5444

General

Start time:	17:15:05
Start date:	03/03/2021
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: 00000007.00000002.275551658.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 6724 Parent PID: 5444

General

Start time:	17:15:05
Start date:	03/03/2021
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: 00000008.00000002.262898420.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EFC	CreateFileA

Analysis Process: WerFault.exe PID: 6844 Parent PID: 6732

General

Start time:	17:15:07
Start date:	03/03/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6732 -s 516
Imagebase:	0xed0000
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	6A951717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D8B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D8B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_29b1fd91934ca85fd856bebf7e23b59544bb3f14_6c16ead4_1afe9588	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_29b1fd91934ca85fd856bebf7e23b59544bb3f14_6c16ead4_1afe9588\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A94497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D8B.tmp	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	success or wait	1	6A944BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	success or wait	1	6A944BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D8B.tmp.xml	success or wait	1	6A944BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC03.tmp.csv	success or wait	1	6A944BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC13.tmp.txt	success or wait	1	6A944BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 9d 34 40 60 a4 05 12 00 00 00 00 00	MDMP..... .....4@`.....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.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 10 18 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 4c 1a 00 00 99 34 40 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 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............ ..GenuineIntelW...........T... ....L....4@`................. ....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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.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 70 3b 00 a2 48 47 00 a2 48 47 00 96 ff 75 cb 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	....+...S...+. ..+....HG..HG..p;..HG..HG.. .u......HG.#...F.......+.........	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	168	50 1a 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 00 00 00 00 00 00 00 00 a2 48 47 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 de 1b 00 00	P........................HG... ....HG.........	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	20	0d 00 00 00 b0 79 56 00 00 00 00 00 04 00 00 00 e2 27 00 00	.....yV..........'..	success or wait	13	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	4	90 fe 91 00	....	success or wait	12	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	4	90 fe 81 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.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 e5 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	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	48	94 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 3c 00 00 00 00 00 c4 fd 91 00 00 00 00 00 3c 02 00 00 7e 4c 00 00 cc 02 00 00 42 24 00 00	....<............ <...~L......B$..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	4	21 00 00 00	!...	success or wait	33	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.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	33	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	752	00 00 a3 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 f4 0e c6 1b 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 f0 3d 02 00 00 00 00 00 a0 b0 02 00 00 00 00 4a 55 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 9d e9 00 00 00 00 00 00 00 7a 54 03 00 00 00 00 00 f4 82 02 00 00 00 00 00 59 24 07 00 00 00 00 00 e7 da 18 00 00 00 00 00 40 ff 1f 00 00 00 00 00 8b e4 18 00 00 00 00	...t.....`..A!..-a..... .....B.....B?..... .....#..... ..@A.....Zb..... ....=..... JU.....zT .....Y$..... @.....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	7556	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 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	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER89A1.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 f0 0d 00 00 9c 07 00 00 05 00 00 00 d4 00 00 00 0e 27 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 b0 14 00 00 52 7c 00 00 15 00 00 00 ec 01 00 00 8c 15 00 00 16 00 00 00 98 00 00 00 78 17 00 00	....'.....T.....8..... ....T.....R|..... .....x...	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.7.3.2.<./.P.i.d.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 35 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.>.4.3.5.2.<./.U.p.t.i.m.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 35 00 37 00 31 00 36 00 39 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.>.8.5.7.1.6.9.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 33 00 39 00 35 00 31 00 36 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.8.3.9.5.1.6.1.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 37 00 33 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.>.1.7.3.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 36 00 37 00 34 00 32 00 30 00 31 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.>.6.7.4.2.0.1.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 36 00 37 00 34 00 32 00 30 00 31 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.>.6.7.4.2.0.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 32 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.2.4.3.2.<./.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 31 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.1.2.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 32 00 31 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.2.1.1.6.8.<./.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 32 00 30 00 38 00 39 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.>.2.0.8.9.6.<./.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 30 00 38 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.7.4.0.8.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 38 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.7.4.8.9.9.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 30 00 38 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.7.4.0.8.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.4.4.<./.P.i.d.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	108	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 35 00 4f 00 38 00 35 00 37 00 36 00 34 00 39 00 30 00 35 00 36 00 33 00 36 00 36 00 34 00 30 00 33 00 30 00 33 00 32 00 30 00 32 00 31 00 2e 00 50 00 44 00 46 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.>.5.O.8.5.7.6.4.9.0.5.6.3.6.6.4.0.3.0.3.2.0.2.1...P.D.F...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 38 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.>.2.5.3.8.2.<./.U.p.t.i.m.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 36 00 31 00 31 00 31 00 35 00 39 00 30 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.>.2.6.1.1.1.5.9.0.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 34 00 38 00 37 00 39 00 39 00 32 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.>.2.4.8.7.9.9.2.3.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 37 00 39 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.7.9.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 37 00 38 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.0.3.7.8.3.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 33 00 33 00 33 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.0.3.3.3.3.3.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.4.2.3.6.9.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 37 00 39 00 38 00 38 00 30 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.>.3.7.9.8.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 39 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.3.3.9.4.4.<./.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P. o.o.l.U.s.a.g.e.>.3.3.1.6.0.<. /.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 35 00 30 00 30 00 36 00 30 00 38 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.>.2.5.0.0.6.0.8.0.<./.P.a.g.e.f. i.l.e.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 31 00 33 00 33 00 30 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.5.1.3.3.0.5.6.<./.P. e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 35 00 30 00 30 00 36 00 30 00 38 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.>.2.5.0.0.6.0.8.0.<./.P.r.i.v.a.t. e.U.s.a.g.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 77 00 67 00 64 00 79 00 6e 00 64 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.>.w.g.d.y.n.d.,. .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	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 77 00 67 00 64 00 79 00 6e 00 64 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.>.w.g.d.y.n.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 37 00 34 00 33 00 37 00 33 00 31 00 34 00 30 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.>.1.5.7.4.3.7.3.1.4.0.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 2d 00 30 00 34 00 54 00 30 00 31 00 3a 00 31 00 35 00 3a 00 31 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.-.0.3.-.0.4.T.0.1.:.1.5.:.1.0.Z.".>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 33 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 36 00 32 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 36 00 32 00 34 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.=.".3.4.3.". .P.I.D.=.".6.7.3.2.". .U.p.t.i.m.e.M.S.=.".1.6.2.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.6.2.4.". .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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 64 00 64 00 65 00 61 00 39 00 64 00 31 00 2d 00 36 00 66 00 30 00 34 00 2d 00 34 00 32 00 38 00 62 00 2d 00 39 00 62 00 37 00 32 00 2d 00 37 00 64 00 31 00 31 00 37 00 33 00 30 00 37 00 64 00 36 00 64 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.5.d.d.e.a.9.d.1.-.6.f.0.4.-.4.2.8.b.-.9.b.7.2.-.7.d.1.1.7.3.0.7.d.6.d.c.<./.G.u.i.d.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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 33 00 2d 00 30 00 34 00 54 00 30 00 31 00 3a 00 31 00 35 00 3a 00 31 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.-.0.3.-.0.4.T.0.1.:.1.5.:.1.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BF4.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	6A94497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D8B.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	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_29b1fd91934ca85fd856bebf7e23b59544bb3f14_6c16ead4_1afe9588\Report.wer	unknown	2	ff fe	..	success or wait	1	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_29b1fd91934ca85fd856bebf7e23b59544bb3f14_6c16ead4_1afe9588\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	164	6A94497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_vbc.exe_29b1fd91934ca85fd856bebf7e23b59544bb3f14_6c16ead4_1afe9588\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 33 00 31 00 38 00 31 00 31 00 35 00 35 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.6.3.1.8.1.1.5.5.0.	success or wait	1	6A94497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	success or wait	1	6A9636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6A961FB2	RegCreateKeyExW
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A9443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	FileId	unicode	0000787d9a6ec3f262e8b71d19ac157c2a286a0f59dd	success or wait	1	6A9636BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	LowerCaseLongPath	unicode	c:\windows\microsoft.net\framework\v2.0.50727\vbc.exe	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	LongPathHash	unicode	vbc.exe|9d6f9af	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Name	unicode	vbc.exe	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Publisher	unicode	microsoft corporation	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Version	unicode	8.0.50727.8922	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	BinFileVersion	unicode	8.0.50727.8922	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	BinaryType	unicode	pe32_i386	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	ProductName	unicode	microsoft. visual studio. 2005	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	ProductVersion	unicode	8.0.50727.8922	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	LinkDate	unicode	02/08/2018 07:12:15	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	BinProductVersion	unicode	8.0.50727.8922	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Size	B	88 E0 11 00 00 00 00 00	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	Language	dword	1033	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	IsPeFile	dword	1	success or wait	1	6A9636BF	unknown
\REGISTRY\A\{c3929724-3cec-e25e-41cf-fe60103a5bb3}\Root\InventoryApplicationFile\vbc.exe|9d6f9af	IsOsComponent	dword	1	success or wait	1	6A9636BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 A2 48 47 00 02 00 00 00 00 00 00 00 A2 48 47 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6A961FE8	RegSetValueExW

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

Disassembly

Code Analysis