ID: 341532
Sample Name: PO 2010029_pdf Quotation from Alibaba Ale.exe
Cookbook: default.jbs
Time: 14:06:23
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

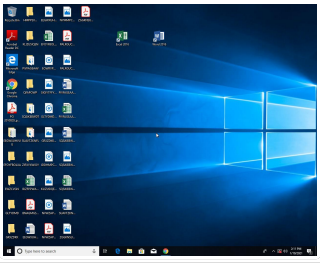
Analysis Report PO 2010029_pdf Quotation from Alibab…

Overview

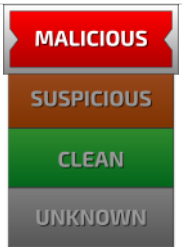
General Information

Sample Name:	PO 2010029_pdf Quotation from Alibaba Ale.exe
Analysis ID:	341532
MD5:	eb59d99961c763..
SHA1:	22d5fb0f076a0d9..
SHA256:	4dd89aea31cfb64.
Tags:	exe Yahoo

Most interesting Screenshot:



Detection



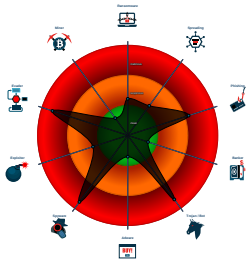
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process…
- Changes the view of files in windows…
- Contains functionality to log keystro…

Classification



Startup

- **System is w10x64**
- PO 2010029_pdf Quotation from Alibaba Ale.exe (PID: 2148 cmdline: 'C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe' MD5: EB59D99961C7636B4872E389DA03CBC9)
  - dw20.exe (PID: 4636 cmdline: dw20.exe -x -s 2216 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
  - vbc.exe (PID: 6084 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
  - vbc.exe (PID: 968 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: 6004 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2148 -s 2244 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- WindowsUpdate.exe (PID: 4848 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: EB59D99961C7636B4872E389DA03CBC9)
- WindowsUpdate.exe (PID: 6328 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: EB59D99961C7636B4872E389DA03CBC9)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b833:$key: HawkEyeKeylogger • 0x7dab7:$salt: 099u787978786 • 0x7be96:$string1: HawkEye_Keylogger • 0x7cce9:$string1: HawkEye_Keylogger • 0x7da17:$string1: HawkEye_Keylogger • 0x7c27f:$string2: holdermail.txt • 0x7c29f:$string2: holdermail.txt • 0x7c1c1:$string3: wallet.dat • 0x7c1d9:$string3: wallet.dat • 0x7c1ef:$string3: wallet.dat • 0x7d5db:$string4: Keylog Records • 0x7d8f3:$string4: Keylog Records • 0x7db0f:$string5: do not script --> • 0x7b81b:$string6: \pidloc.txt • 0x7b8a9:$string7: BSPLIT • 0x7b8b9:$string7: BSPLIT
00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x7beee:$hawkstr1: HawkEye Keylogger • 0x7cd2f:$hawkstr1: HawkEye Keylogger • 0x7d05e:$hawkstr1: HawkEye Keylogger • 0x7d1b9:$hawkstr1: HawkEye Keylogger • 0x7d31c:$hawkstr1: HawkEye Keylogger • 0x7d5b3:$hawkstr1: HawkEye Keylogger • 0x7ba7c:$hawkstr2: Dear HawkEye Customers! • 0x7d0b1:$hawkstr2: Dear HawkEye Customers! • 0x7d208:$hawkstr2: Dear HawkEye Customers! • 0x7d36f:$hawkstr2: Dear HawkEye Customers! • 0x7bb9d:$hawkstr3: HawkEye Logger Details:
Click to see the 91 entries				

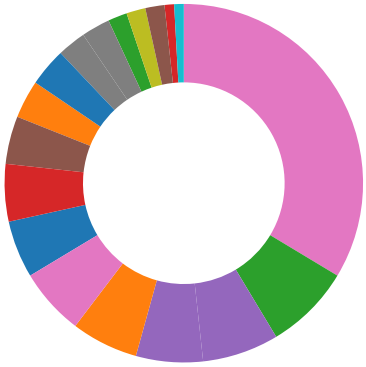
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.ad0000.1.unpack	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x58eb7:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x5883f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34
11.2.WindowsUpdate.exe.1c5f0000.3.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x8908b:$key: HawkEyeKeylogger • 0x8b30f:$salt: 099u787978786 • 0x896ee:$string1: HawkEye_Keylogger • 0x8a541:$string1: HawkEye_Keylogger • 0x8b26f:$string1: HawkEye_Keylogger • 0x89ad7:$string2: holdermail.txt • 0x89af7:$string2: holdermail.txt • 0x89a19:$string3: wallet.dat • 0x89a31:$string3: wallet.dat • 0x89a47:$string3: wallet.dat • 0x8ae33:$string4: Keylog Records • 0x8b14b:$string4: Keylog Records • 0x8b367:$string5: do not script --> • 0x89073:$string6: \pidloc.txt • 0x89101:$string7: BSPLIT • 0x89111:$string7: BSPLIT
11.2.WindowsUpdate.exe.1c5f0000.3.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
11.2.WindowsUpdate.exe.1c5f0000.3.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 110 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

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

Binary contains paths to debug symbols

Networking:

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

Installs a global keyboard hook

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:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

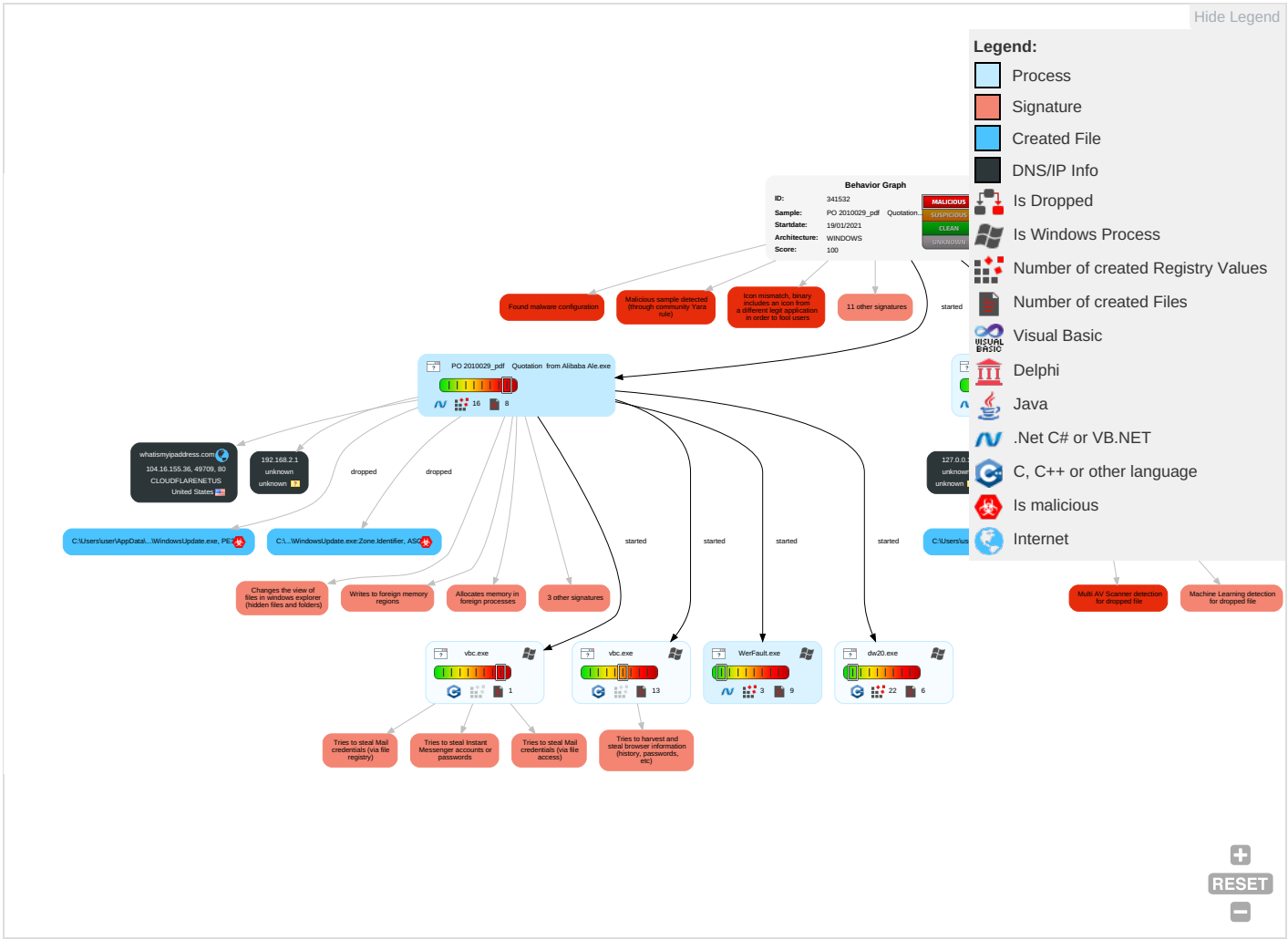
Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Othe Network Medium
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 1	Process Injection 4 1 1	Obfuscated Files or Information 3	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltratio
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 3 8	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Security Software Discovery 1 6 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypte Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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/Obfusca Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

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
PO 2010029_pdf Quotation from Alibaba Ale.exe	37%	ReversingLabs	Win32.Backdoor.NanoBot	
PO 2010029_pdf Quotation from Alibaba Ale.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	37%	ReversingLabs	Win32.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.WindowsUpdate.exe.ed0000.1.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
3.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
11.2.WindowsUpdate.exe.1ee40000.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
8.2.WindowsUpdate.exe.1c5f0000.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.ad0000.1.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.PO 2010029_pdf Quotation from Alibaba Ale.exe.ad0000.0.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
8.2.WindowsUpdate.exe.1ad90000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
8.2.WindowsUpdate.exe.1ad90000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
11.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
8.2.WindowsUpdate.exe.ed0000.1.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
11.2.WindowsUpdate.exe.1c5f0000.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
8.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
8.2.WindowsUpdate.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1efe0000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1efe0000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1c6f0000.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
8.0.WindowsUpdate.exe.ed0000.0.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
0.2.PO 2010029_pdf Quotation from Alibaba Ale.exe.1ef40000.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
11.2.WindowsUpdate.exe.1eed0000.5.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
11.2.WindowsUpdate.exe.1eed0000.5.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.WindowsUpdate.exe.ed0000.0.unpack	100%	Avira	HEUR/AGEN.1138127		Download File
8.2.WindowsUpdate.exe.1ee00000.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.com.12	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnBm	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comItaf	0%	Avira URL Cloud	safe	
http://foo.com/fooT	0%	Avira URL Cloud	safe	
http://www.carterandcone.comeci	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comceco	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://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comypo	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.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	

Source	Detection	Scanner	Label	Link
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.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.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.founder.com.cn/cnxmQ	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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.comitk.	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.founder.com.cn/cn(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

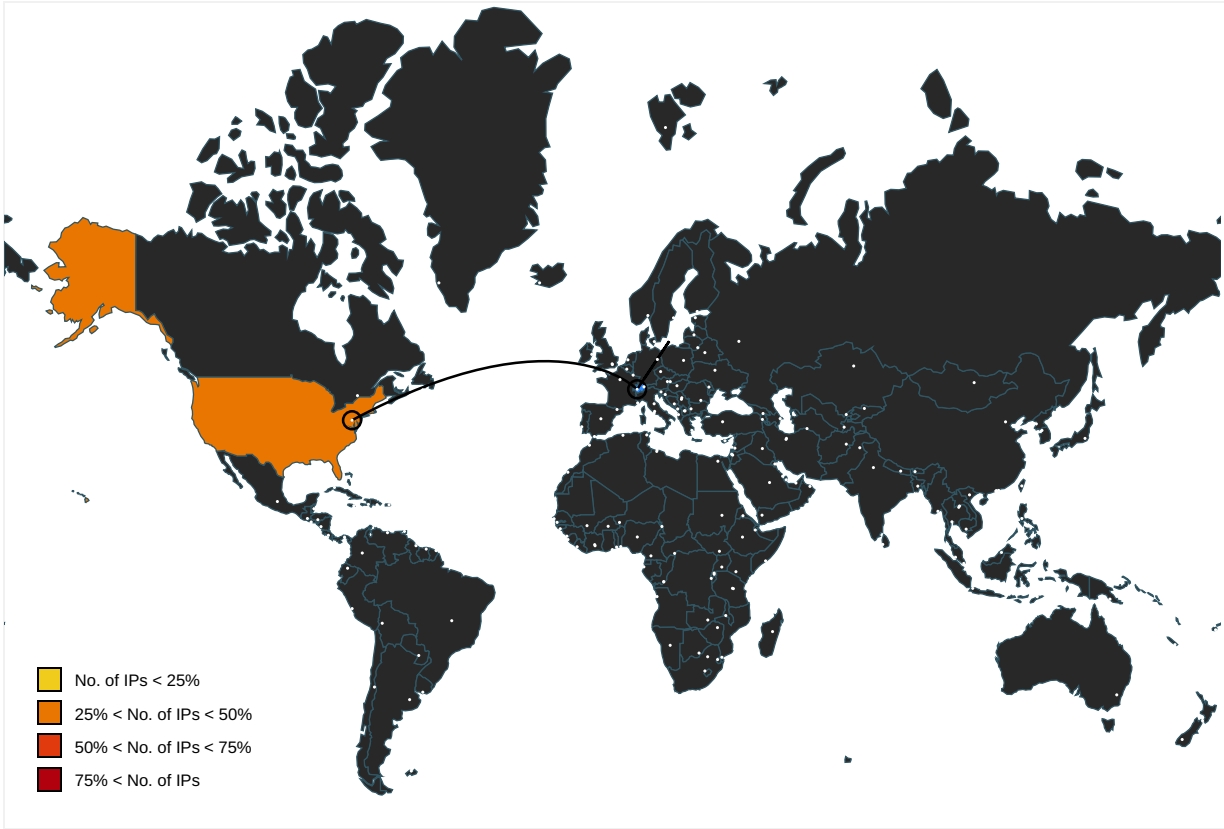
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.carterandcone.com.12	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.223629764.000000001F138000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317281962.000000001F120000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnBm	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.222855521.000000001F152000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comItaf	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.223629764.000000001F138000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://foo.com/fooT	WindowsUpdate.exe, 00000008.00000002.308158001.000000001CC12000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000000B.00000002.312377035.000000001CCB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comeci	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.223629764.000000001F138000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersB	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.228030667.000000001F12D000.00000004.00000001.sdmp	false		high
http://www.tiro.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://whatismyipaddress.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.313417162.000000001CCF1000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comceco	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317281962.000000001F120000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp, PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.228030667.000000001F12D000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.223535347.000000001F138000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.222007881.000000001F12D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comypo	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.223629764.000000001F138000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.monotype.	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.227248438.000000001F12F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnxmQ	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.222855521.000000001F152000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://whatismyipaddress.com/-	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.316835361.000000001DCF1000.00000004.00000001.sdmp, WindowsUpdate.exe, 00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp, WindowsUpdate.exe, 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.224519756.000000001F137000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	WindowsUpdate.exe	false		high
http://www.fonts.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comalic	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317281962.000000001F120000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	WindowsUpdate.exe, 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comitk.	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.223535347.000000001F138000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000002.317453803.000000001F290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn(	PO 2010029_pdf Quotation from Alibaba Ale.exe, 00000000.00000003.222855521.000000001F152000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341532
Start date:	19.01.2021
Start time:	14:06:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO 2010029_pdf Quotation from Alibaba Ale.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:	34
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@10/13@1/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.7% (good quality ratio 10.9%) • Quality average: 77.3% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 96% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, HxTsr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 2.18.68.82, 51.11.168.160, 2.20.142.210, 2.20.142.209, 51.103.5.186, 92.122.213.201, 92.122.213.247, 20.54.26.129, 40.88.32.150, 168.61.161.212, 51.104.144.132, 51.104.139.180, 52.254.96.93, 52.251.11.100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:08:16	API Interceptor	6x Sleep call for process: PO 2010029_pdf Quotation from Alibaba Ale.exe modified
14:08:20	API Interceptor	1x Sleep call for process: dw20.exe modified
14:08:21	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
14:08:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
14:08:48	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NXmokFkh3R.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	qiGQsdRM57.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NSSPH41vE5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• 104.16.155.36
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• 104.16.155.36
	B6LNCKjOGt5EmFQ.exe	Get hash	malicious	Browse	• 104.16.154.36
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• 104.16.155.36
	JkhR5oeRHA.exe	Get hash	malicious	Browse	• 66.171.248.178
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• 104.16.154.36
	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	khJdbt0clZ.exe	Get hash	malicious	Browse	• 104.16.154.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• 104.16.154.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	January RFQ..exe	Get hash	malicious	Browse	• 23.227.38.74
	SKM_C221200706052800n.exe	Get hash	malicious	Browse	• 66.235.200.146
	KuPBIsrqbO.exe	Get hash	malicious	Browse	• 23.227.38.74
	RrZ6BOnPCG.exe	Get hash	malicious	Browse	• 104.21.27.226
	Fdj5vhj87S.exe	Get hash	malicious	Browse	• 104.16.186.173
	INV0009876.exe	Get hash	malicious	Browse	• 104.21.19.200
	00000000987772021.exe	Get hash	malicious	Browse	• 172.67.188.154
	_MVSEASEAL_RFQ_.xlsx	Get hash	malicious	Browse	• 104.16.186.173
	Invoice Payment Details.exe	Get hash	malicious	Browse	• 66.235.200.147
	invoice68684881.xls	Get hash	malicious	Browse	• 162.159.134.233
	invoice68684881.xls	Get hash	malicious	Browse	• 162.159.135.233
	RFQ_FOR_PO.exe	Get hash	malicious	Browse	• 172.67.188.154
	1_cr.exe	Get hash	malicious	Browse	• 172.67.219.133
	PaySlip140121.xls	Get hash	malicious	Browse	• 162.159.135.233
	RFQ (2).exe	Get hash	malicious	Browse	• 172.67.188.154
	1_cr.exe	Get hash	malicious	Browse	• 104.21.45.223
	PaySlip140121.xls	Get hash	malicious	Browse	• 104.22.1.232
	TT Slip.doc	Get hash	malicious	Browse	• 162.159.133.233
	n#U00b0761.xls	Get hash	malicious	Browse	• 162.159.133.233
	Shipment ConfirmationPaper - Customer Copy_pdf.exe	Get hash	malicious	Browse	• 172.67.219.133

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_I3UYUDMLOPVYGRAZ_7057fda4f89bb183663b41fd976febdf70a304b_00000000_124dc6e0\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18018
Entropy (8bit):	3.7671072989618524
Encrypted:	false
SSDEEP:	192:7VE5vnFWMhV203jZIhy9UcJN5X5Q17zvMvkvDKGwNYeh/u7sfS274lt0z:RInFNljzqv3vOh/u7sfX4ltl
MD5:	5A930DC669FC64A68231E3F0739BF7A2
SHA1:	2ADA755AAC4C1AAE4C6154EA8E503A5F1CAF49A5
SHA-256:	7CC51741A64901D2FB0BFAC502C42FAD2F109FE005831BACB958E6663483437F
SHA-512:	63D374183C0D9F0A68EF7E46ED2D0DD7654C1B014719C3EDF176DB3CA069DD41BB4559A3C5F78A90C84E6113674D8D43C8CB034BC6E4AAEAC333588A9AF3D1D
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.5.6.7.6.9.7.8.2.0.1.6.8.1.....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.=.1.3.2.5.5.5.6.7.6.9.8.2.1.0.7.9.4.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.5.4.d.f.8.f.d.-.5.6.f.9.-.4.a.c.c.-.b.0.3.f.-.6.e.1.7.2.3.3.4.6.6.3.c.....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.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.6.4.-.0.0.0.1.-.0.0.1.7.-.a.1.1.e.-.0.1.9.3.a.f.e.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.c.5.e.b.d.5.8.d.1.9.3.3.b.e.2.9.b.8.8.7.2.0.2.0.b.9.e.c.0.5.8.0.0.0.0.f.f.f.f.!.0.0.0.0.2.2.d.5.f.b.0.f.0.7.6.a.0.d.9.4.5.5.9.6.b.7.9.3.8.e.7.2.b.6.b.5.c.a.e.7.3.6.7.4.!.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.n. . .f.r.o.m. .A.l.i.b.a.b.a. .A.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.1././.1.8.:.2.0.:.2.8.:.2.0.!.0.!.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO 2010029_pdf _72613674f79bb87c1b11e7d393fe053666d79f1_6467c67c_1726352a\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	19162
Entropy (8bit):	3.773653319477634
Encrypted:	false
SSDEEP:	192:d3q5vWeHBUZMXj03jZIhy9UcJN5X5Q17zvMvkvDKGwNYeSTs/u7sES274ItihBG:opBUZMX4jzqv3vOS4/u7sEX4ItEG
MD5:	794BD95DB4ACDF7A0AB11BA3AB6CA638
SHA1:	081C01144CD21C704C0B0138BC64D81AE3B70B64
SHA-256:	4F64768EAF8E951A12B5269ECC5F3D26D228131F504700375153376BB14C3571
SHA-512:	13F3123264DCA07F3DB79D69408444CD823287AF8CA1EF6E0C72AFCF4391B951C462491E21FEAB3C48747BA92B2DE11BF89EEE1977F09A6E9F20BF4A9B910AA9
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.=.1.3.2.5.5.5.6.7.7.0.3.7.4.2.0.2.8.3.....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.=.1.3.2.5.5.5.6.7.7.0.9.7.4.2.0.1.0.1.....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.=.9.6.c.c.a.1.2.4.-.a.5.b.c.-.4.e.3.9.-.b.c.e.f.-.4.a.f.5.5.e.0.8.7.f.7.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.=.2.9.d.9.9.5.c.c.-.5.c.7.5.-.4.c.6.9.-.9.3.6.0.-.7.4.6.b.6.9.5.4.3.b.6.2.....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.=.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.n. . .f.r.o.m. .A.l.i.b.a.b.a. .A.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.6.4.-.0.0.0.1.-.0.0.1.7.-.a.1.1.e.-.0.1.9.3.a.f.e.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.c.5.e.b.d.5.8.d.1.9.3.3.b.e.2.9.b.8.8.7.2.0.2.0.b.9.e.c.0.5.8.0.0.0.0.f.f.f.f.!.0.0.0.0.2.2.d.5.f.b.0.f.0.7.6.a.0.d.9.4.5.5.9.6.b.7.9.3.8.e.7.2.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB95.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7786
Entropy (8bit):	3.712017053076674
Encrypted:	false
SSDEEP:	192:RrI7r3GLNihCx6yo6YSBmSUDMvgmfZ4OQSkCp1Lng1f45m:RrlsNiy6yo6YlSUDMvgmfGOQSNLnqfr
MD5:	84CEF630CF0681BFAFF5795DCD1DD9BF
SHA1:	20DAFD24F4C7DAF6F9E08DFB388E77B66F11C49B
SHA-256:	343A0751D0B019585B5A655031941A406CBF403CDDF33498853B1536B7B287D9
SHA-512:	15273848255FFACC787D724ADD047C34B1B0BEFE0BB86983E397E0B8E26676BD54046D8D8A5516D3ADC1195D4B528BBDD0A93D8FB7A18A182567A730E36F314
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.>.2.1.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBC61.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4727
Entropy (8bit):	4.5249078201260895
Encrypted:	false
SSDEEP:	48:cvIwSD8zsiJgtWI99NeyWSC8B58/8fm8M4JFKnEFK+q8vIMpyzpz43d:uITfwaQTSNX8kJFKvK7pMBGd
MD5:	A77D974765EA039F1262BFEFC930DDD0
SHA1:	BD9A0C9A7E2125EC668643A67C1DE5AB7053BEE9
SHA-256:	EBE9C543D0C54888E69F73621631DF24BCF7996158CC4F69805CB448B11CF2EF
SHA-512:	3BCC218C23C2DC2E44752FA14AC1FA69DB851ABD518D3A3D0AE43FFB3B4563C39273E7FC4C473ECB3DC85CA505A18F61F7489744E541C6AE8D513ECF9BB6FC0
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="824118" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	
File Type:	Mini DuMP crash report, 14 streams, Tue Jan 19 22:08:25 2021, 0x60521 type
Category:	dropped
Size (bytes):	6933739
Entropy (8bit):	4.734653460543801
Encrypted:	false
SSDEEP:	98304:QaMVHrkZq8y7Lb1XaMynrEh+9Hqt+G/haJly0c83ruYGvkKPTIs:fMVQZN8EnrEh+9HxIqRkKUs
MD5:	0FFA20CF1EEC67FD898D3AC64D6C7231
SHA1:	8C3CF535A2A1CB827A54C03E639186B21075957A
SHA-256:	1646FD0EA566759E195DE0B910D4C301D02FD7D8B9BDE02629FA575AA885DD11
SHA-512:	95EE59C890A3C14B7A3DE35A984495ACEB0D859BB7F63BF5860D9CD5382A3BE7787056C79BBA6D2DDF29B77E559248C36006829E4FEBEDB46ABFEE45B64F7551
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....YX.`!.....U.....B.....7.....GenuineIntelW.....T.....d...JX.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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):	8524
Entropy (8bit):	3.7080535077803924
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNihCRl656YShSUvThRgmfVTSTCprs89bPnosftFm:RrlsNio656YUSUvThRgmfBSCPnbfu
MD5:	9FB20031D8273F271E0B02DC2888B81C
SHA1:	6C03A55C542379A201F850452865CD8F567A0890
SHA-256:	5B1B04CE45984D2003633B3BFD590A9331B4A5AC320A5503CD7CCA1AFFDE54F6
SHA-512:	4994B1FA03EDAB8B6DA865A1BB741A6E8868542289F737210B4797FC188CFE1D0BEC636E20296971C3526760BDB864350D35DD2047F15E360F1FB066B891596D
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.>.2.1.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1CC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.5195633541037825
Encrypted:	false
SSDEEP:	48:cvIwSD8zspJgtWI99NeyWSC8BB8fm8M4JwO5mEZFJV+q8GqUlpyzpz4Ed:uITf7aQTSNkJwktVJlpMBVd
MD5:	8EDDFB7B4C01B2217653133720FB0C3E
SHA1:	EE64A9AD9FA38CD71213C86424622FFAC7D57030
SHA-256:	684425CEB1CC7C1C95D447C778B60281477DD85DC2083EA402C13C61E74498B2
SHA-512:	40C7AA1A2B7B031FE823E3D4619D87F05A7B7B96981B46716DC113A194668A1B1212500D6C1FB5E087DAFBC0800517A53E017FF0B6BDD3BCF014A57F89A7E53
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="824119" />.. <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_v2.0_32\UsageLogs\WindowsUpdate.exe.log	
Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EE FF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a909923 7864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System .Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1074688
Entropy (8bit):	7.570804768501044
Encrypted:	false
SSDEEP:	12288:f8WvAMYGY5RFNBeU7vgTOzcdCeddAAU8f9MkdPUBphp5wvvXLlweomEL+wif7APY:f8W4T17vgKzYXAm+DfuTXomAuzABdpu
MD5:	EB59D99961C7636B4872E389DA03CBC9
SHA1:	22D5FB0F076A0D945596B7938E72B6B5CAE73674
SHA-256:	4DD89AEA31CFB64C8FA6B542C9AD002E4041EF5249F2072947DF749E00E7FD9E
SHA-512:	6D062B65284DF0F4CE5845B8730AC6ADF46759AF5F35E3BDE86A609BCE9FF0D5846FBE2D30864E411B695D774B6F6903D558E42F067C44817E3421CD5D41B25
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...|..|..|.....v.....n..._#.....o....a.....n.....m..|.....}.....}....}..Rich|.... .....PE..L...d..`.....@.....`.....@.....F..... .....0..<,...6.....06..@.....`..... .....text...:..... ..`.rdata.....@..@.data...4....`.....B.....@....gfids..t.....N.....@..@.rsrc... .....P.....@..@.reloc..<,...0..... .....@..B..... .....

C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:Q:Q
MD5:	E21E4E58AD9AB56E8A4634046DA90113
SHA1:	D7C1F0DD609C0024D00C7EB35743BCC476459876
SHA-256:	2C6499976963E9832529BC8D9DFF516D16C13D372D852D1500F5892E46A25507
SHA-512:	0A18737EFF8DEE2E701D7F75B10A56E5610AC75D379E0D4D5528ADADE8D7367618FAFDFEB9F16B66C36DAF4A152D96DCFE9E0B5B47A4CEBB6FDAD6A19FDB9134
Malicious:	false
Preview:	2148

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.792723397330207
Encrypted:	false
SSDEEP:	3:oNWXp5v1qOL/kiRMQFLTzxl0C:oNWXpFgOLHXLvxl0C
MD5:	C2645D3F71F5EA8326BA0B900632630D
SHA1:	0456DB88ECD2D46E89CDCFD159029FA44E10B928
SHA-256:	92283FB25F70604C5445F52AD17CFC2E7F206C63D5F737B8A81F12F1FC73BB19
SHA-512:	0DBE031016D3A882000116A853F4D8FC463AF466948781AE816349878577B4C67ADE9AA0F96D2B0C7E513C3D8536E0D46CD63B417F802E7E01CA064426823881
Malicious:	false
Preview:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.570804768501044
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO 2010029_pdf Quotation from Alibaba Ale.exe
File size:	1074688
MD5:	eb59d99961c7636b4872e389da03cbc9
SHA1:	22d5fb0f076a0d945596b7938e72b6b5cae73674
SHA256:	4dd89aea31cfb64c8fa6b542c9ad002e4041ef5249f2072947df749e00e7fd9e
SHA512:	6d062b65284df0f4ce5845b8730ac6adf46759af5f35e3bde86a609bce9ff0d5846fbe2d30864e411b695d774b6f6903d558e42f067c44817e3421cd5d41b256
SSDEEP:	12288:f8WvAMYGY5RFNBeU7vgTOzcdCeddAAU8f9MkdPUBphp5wvvXLlweomEL+wif7APY:f8W4T17vgKzYXAm+DfuTXomAuzABdpu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...|...|...|.....v.....n...._#.....o.....a.....n.....m...|.....}.....}.....}...Rich|.....

File Icon

Icon Hash:	6eeccccd6d2f2f2

Static PE Info

General

Entrypoint:	0x401308
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6005EF64 [Mon Jan 18 20:28:20 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	3f85ebb67bac58f72de974a91d40889a

Entrypoint Preview

Instruction
call 00007FA3F8CD8798h
jmp 00007FA3F8CD8255h
push 00000014h
push 00453B58h
call 00007FA3F8CD8AE7h
push 00000001h
call 00007FA3F8CD8560h
pop ecx
test al, al
jne 00007FA3F8CD8259h
push 00000007h
call 00007FA3F8CD8887h
xor bl, bl
mov byte ptr [ebp-19h], bl
and dword ptr [ebp-04h], 00000000h
call 00007FA3F8CD8449h
mov byte ptr [ebp-24h], al
mov eax, dword ptr [00456A80h]
xor ecx, ecx
inc ecx
cmp eax, ecx
je 00007FA3F8CD822Eh
test eax, eax
jne 00007FA3F8CD829Bh
mov dword ptr [00456A80h], ecx
push 0044B290h
push 0044B270h
call 00007FA3F8CF96BFh
pop ecx
pop ecx
test eax, eax
je 00007FA3F8CD8263h
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, 000000FFh
jmp 00007FA3F8CD834Bh

Instruction
push 0044B26Ch
push 0044B264h
call 00007FA3F8CF963Dh
pop ecx
pop ecx
mov dword ptr [00456A80h], 00000002h
jmp 00007FA3F8CD8257h
mov bl, cl
mov byte ptr [ebp-19h], bl
push dword ptr [ebp-24h]
call 00007FA3F8CD8637h
pop ecx
call 00007FA3F8CD87FEh
mov esi, eax
xor edi, edi
cmp dword ptr [esi], edi
je 00007FA3F8CD826Ch
push esi
call 00007FA3F8CD8599h
pop ecx
test al, al
je 00007FA3F8CD8261h
push edi
push 00000002h
push edi
mov esi, dword ptr [esi]
mov ecx, esi
call 00007FA3F8CD8A27h
call esi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x546dc	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x59000	0x19f20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x73000	0x2c3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x53610	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x53630	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4b000	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4993a	0x49a00	False	0.472009629669	data	6.6152740435	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4b000	0xa3aa	0xa400	False	0.45107660061	SysEx File - Mesosha	5.23997613425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x1f34	0xc00	False	0.171549479167	DOS executable (block device driver \277DN)	2.22955442271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x58000	0x174	0x200	False	0.341796875	data	2.11448669888	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x59000	0x19f20	0x1a000	False	0.195575420673	data	4.62816449784	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x73000	0x2c3c	0x2e00	False	0.783882472826	data	6.63145431335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x591c0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x5b768	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x5c810	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x5cc78	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x60ea0	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_RCDATA	0x71718	0x1805	data	English	United States
RT_GROUP_ICON	0x716c8	0x4c	data	English	United States

Imports

DLL	Import
KERNEL32.dll	Heap32Next, LoadResource, FreeLibrary, GetLongPathNameA, CancelIo, BuildCommDCBAndTimeoutsA, ExitThread, GlobalFindAtomW, GetStdHandle, HeapAlloc, GetProcessHeap, SetConsoleCursorPosition, DecodePointer, EncodePointer, SetEndOfFile, WriteConsoleW, HeapReAlloc, HeapSize, GetTimeZoneInformation, SetConsoleMode, ReadConsoleInputW, ReadConsoleInputA, PeekConsoleInputA, GetNumberOfConsoleInputEvents, CreateFileW, SetConsoleCtrlHandler, GetStringTypeW, SetStdHandle, SetEnvironmentVariableW, SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetCPInfo, GetOEMCP, IsValidCodePage, FindNextFileW, FindNextFileA, FindFirstFileExW, FindFirstFileExA, FindClose, MoveFileExW, GetFileAttributesExW, CreateProcessW, CreateProcessA, GetExitCodeProcess, WaitForSingleObject, GetCurrentThread, DeleteFileW, CloseHandle, GetConsoleCP, FlushFileBuffers, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, GetCurrentProcess, TerminateProcess, InterlockedPushEntrySList, InterlockedFlushSList, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, ReadFile, QueryPerformanceFrequency, MultiByteToWideChar, WriteFile, GetModuleFileNameW, GetModuleFileNameA, WideCharToMultiByte, GetACP, HeapFree, SetFilePointerEx, GetConsoleMode, ReadConsoleW, GetFileType, OutputDebugStringA, OutputDebugStringW, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, RaiseException
SHELL32.dll	DragQueryFile, Shell_NotifyIconA
MSWSOCK.dll	EnumProtocolsA, GetNameByTypeW, GetServiceA, getnetbyname
mscms.dll	EnumColorProfilesW, UnregisterCMMA, CreateProfileFromLogColorSpaceW, GetPS2ColorRenderingIntent, EnumColorProfilesA
msi.dll	
WS2_32.dll	gethostbyaddr, WSCInstallNameSpace, WSALookupServiceNextA, WSARemoveServiceClass
ODBC32.dll	VRetrieveDriverErrorsRowCol
USER32.dll	GetDC, GrayStringW

Possible Origin

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

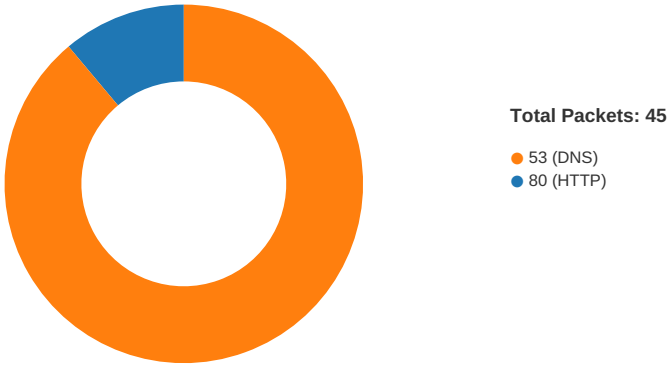
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/19/21-14:07:24.893873	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49709	104.16.155.36	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:07:24.803280115 CET	49709	80	192.168.2.3	104.16.155.36
Jan 19, 2021 14:07:24.843286991 CET	80	49709	104.16.155.36	192.168.2.3
Jan 19, 2021 14:07:24.843444109 CET	49709	80	192.168.2.3	104.16.155.36
Jan 19, 2021 14:07:24.844419956 CET	49709	80	192.168.2.3	104.16.155.36
Jan 19, 2021 14:07:24.884332895 CET	80	49709	104.16.155.36	192.168.2.3
Jan 19, 2021 14:07:24.893872976 CET	80	49709	104.16.155.36	192.168.2.3
Jan 19, 2021 14:07:24.944005013 CET	49709	80	192.168.2.3	104.16.155.36
Jan 19, 2021 14:08:07.401418924 CET	49709	80	192.168.2.3	104.16.155.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:07:24.737133026 CET	50620	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:24.784964085 CET	53	50620	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:27.024379015 CET	64938	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:27.080846071 CET	53	64938	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:29.446954966 CET	60152	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:29.503288984 CET	53	60152	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:38.352360964 CET	57544	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:38.406651974 CET	55984	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:38.416496992 CET	53	57544	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:38.465986013 CET	53	55984	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:41.692348957 CET	64185	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:41.777007103 CET	53	64185	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:46.849670887 CET	65110	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:46.898314953 CET	53	65110	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:53.292752028 CET	58361	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:07:53.342840910 CET	53	58361	8.8.8.8	192.168.2.3
Jan 19, 2021 14:07:59.963716030 CET	63492	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:00.014316082 CET	53	63492	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:02.032809973 CET	60831	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:02.093347073 CET	53	60831	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:04.101022005 CET	60100	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:04.151834011 CET	53	60100	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:11.430254936 CET	53195	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:11.486526012 CET	53	53195	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:11.658313990 CET	50141	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:11.719221115 CET	53	50141	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:08:12.349411964 CET	53023	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:12.397241116 CET	53	53023	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:13.509324074 CET	49563	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:13.557267904 CET	53	49563	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:19.087261915 CET	51352	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:19.135039091 CET	53	51352	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:20.055285931 CET	59349	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:20.111741066 CET	53	59349	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:21.066859961 CET	57084	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:21.114937067 CET	53	57084	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:27.746773005 CET	58823	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:27.794595957 CET	53	58823	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:31.018626928 CET	57568	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:31.066662073 CET	53	57568	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:33.980485916 CET	50540	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:34.031049013 CET	53	50540	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:37.069364071 CET	54366	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:37.125648975 CET	53	54366	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:42.337563992 CET	53034	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:42.385427952 CET	53	53034	8.8.8.8	192.168.2.3
Jan 19, 2021 14:08:42.811871052 CET	57762	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:08:42.859744072 CET	53	57762	8.8.8.8	192.168.2.3
Jan 19, 2021 14:09:08.177627087 CET	55435	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:09:08.225469112 CET	53	55435	8.8.8.8	192.168.2.3
Jan 19, 2021 14:09:09.648237944 CET	50713	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:09:09.699141026 CET	53	50713	8.8.8.8	192.168.2.3
Jan 19, 2021 14:09:41.623981953 CET	56132	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:09:41.674923897 CET	53	56132	8.8.8.8	192.168.2.3
Jan 19, 2021 14:09:59.172621965 CET	58987	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:09:59.220423937 CET	53	58987	8.8.8.8	192.168.2.3
Jan 19, 2021 14:09:59.894496918 CET	56579	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:09:59.951042891 CET	53	56579	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:03.218694925 CET	60633	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:03.275172949 CET	53	60633	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:03.438195944 CET	61292	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:03.494326115 CET	53	61292	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:04.525226116 CET	63619	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:04.587599993 CET	53	63619	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:05.257047892 CET	64938	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:05.313369989 CET	53	64938	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:05.526376009 CET	61946	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:05.585340977 CET	53	61946	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:06.657068968 CET	64910	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:06.705086946 CET	53	64910	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:07.892919064 CET	52123	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:07.952100992 CET	53	52123	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:09.728214979 CET	56130	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:10.763556004 CET	56130	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:11.809860945 CET	56130	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:11.873954058 CET	53	56130	8.8.8.8	192.168.2.3
Jan 19, 2021 14:10:13.257555962 CET	56338	53	192.168.2.3	8.8.8.8
Jan 19, 2021 14:10:13.315814018 CET	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 14:07:24.737133026 CET	192.168.2.3	8.8.8.8	0x8b8d	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 14:07:24.784964085 CET	8.8.8.8	192.168.2.3	0x8b8d	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 14:07:24.784964085 CET	8.8.8.8	192.168.2.3	0x8b8d	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

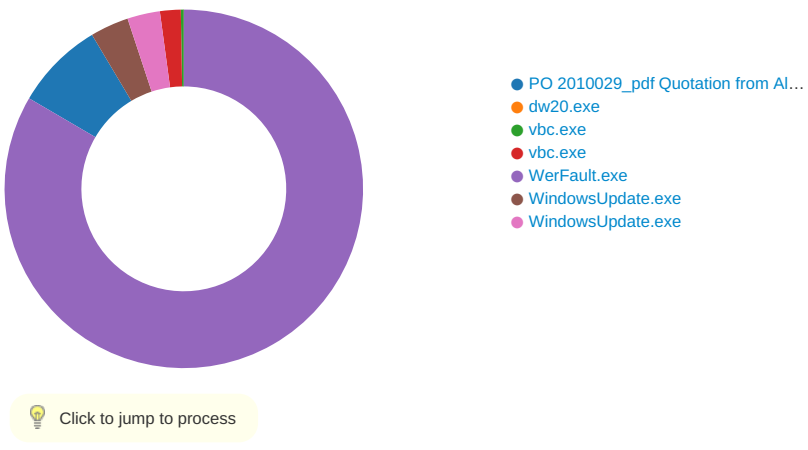
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49709	104.16.155.36	80	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 14:07:24.844419956 CET	0	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Jan 19, 2021 14:07:24.893872976 CET	1	IN	HTTP/1.1 403 Forbidden Date: Tue, 19 Jan 2021 13:07:24 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Set-Cookie: __cfduid=dc5c380c1a5d92fcf9cb84a16088ebe551611061644; expires=Thu, 18-Feb-21 13:07:24 GMT; path=/; domain=.whatismyipaddress.com; HttpOnly; SameSite=Lax; Secure cf-request-id: 07bc5ae64d0000d711d12b6000000001 Server: cloudflare CF-RAY: 6140c7507a92d711-FRA Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO 2010029_pdf Quotation from Alibaba Ale.exe PID: 2148 Parent PID: 5704

General

Start time:	14:08:10
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe'
Imagebase:	0xad0000
File size:	1074688 bytes
MD5 hash:	EB59D99961C7636B4872E389DA03CBC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.316835361.000000001DCF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.316835361.000000001DCF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.316835361.000000001DCF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.316835361.000000001DCF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.316835361.000000001DCF1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.301261564.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.301261564.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.301261564.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.301261564.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.301261564.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.317001771.000000001EEAE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.317001771.000000001EEAE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.317001771.000000001EEAE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.317001771.000000001EEAE000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.317001771.000000001EEAE000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.317140638.000000001EFE2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.317140638.000000001EFE2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.317140638.000000001EFE2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.317140638.000000001EFE2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.317140638.000000001EFE2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.317057911.000000001EF40000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.317057911.000000001EF40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.317057911.000000001EF40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.317057911.000000001EF40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.317057911.000000001EF40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.311897650.000000001C6F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.311897650.000000001C6F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.311897650.000000001C6F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.311897650.000000001C6F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.311897650.000000001C6F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.313417162.000000001CCF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.313417162.000000001CCF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.313417162.000000001CCF1000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	1C79BDFF	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	1C79BDFF	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1AEF4F28	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	1AEF4F28	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	1AEF5CCA	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	1AEF5CCA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	32 31 34 38	2148	success or wait	1	1AEF0163	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	72	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 50 4f 20 32 30 31 30 30 32 39 5f 70 64 66 20 20 20 20 51 75 6f 74 61 74 69 6f 6e 20 20 66 72 6f 6d 20 41 6c 69 62 61 62 61 20 41 6c 65 2e 65 78 65	C:\Users\user\Desktop\PO 2010029_pdf Quotation from Alibaba Ale.exe	success or wait	1	1AEF0163	WriteFile
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 38 9e 8a d9 7c ff e4 8a 7c ff e4 8a 7c ff e4 8a 0f 9d e7 8b 76 ff e4 8a 0f 9d e1 8b ce ff e4 8a 0f 9d e0 8b 6e ff e4 8a e2 5f 23 8a 7f ff e4 8a d1 a1 e7 8b 6f ff e4 8a d1 a1 e1 8b 61 ff e4 8a d1 a1 e0 8b 6e ff e4 8a 0f 9d e5 8b 6d ff e4 8a 7c ff e5 8a ec ff e4 8a c9 a1 ec 8b 7d ff e4 8a c9 a1 1b 8a 7d ff e4 8a c9 a1 e6 8b 7d ff e4 8a 52 69 63 68 7c ff e4 8a 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....8...|...|...|.....v. .....n...._#..... o.....a.....n.....m...|. .....}.....}.....}... Rich|.....	success or wait	5	1AEF4F28	CopyFileW
C:\Users\user\AppData\Roaming\ WindowsUpdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	1AEF4F28	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1AEF0163	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1AEF0163	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	1AEF0163	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	1AEF0163	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	1AEF0163	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Windows Update	unicode	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	1AEF5102	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	1AEF49BE	RegSetValueExW

Analysis Process: dw20.exe PID: 4636 Parent PID: 2148

General

Start time:	14:08:17
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2216
Imagebase:	0x7ff6741d0000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: vbc.exe PID: 6084 Parent PID: 2148

General

Start time:	14:08:20
Start date:	19/01/2021
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: 00000002.00000002.240465103.0000000000400000.00000040.00000001.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: vbc.exe PID: 968 Parent PID: 2148

General

Start time:	14:08:20
Start date:	19/01/2021
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: 00000003.00000002.245754614.0000000000400000.00000040.00000001.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\holderwb.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407175	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	2	ff fe	..	success or wait	1	407BCF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	414E52	ReadFile

Analysis Process: WerFault.exe PID: 6004 Parent PID: 2148

General

Start time:	14:08:22
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2148 -s 2244
Imagebase:	0xe50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D5A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1CC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1CC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO2010029_pdf _72613674f79bb87c1b11e7d393fe053666d79f1_6467c67c_1726352a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO2010029_pdf _72613674f79bb87c1b11e7d393fe053666d79f1_6467c67c_1726352a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D59497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1CC.tmp	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	success or wait	1	6D594BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	success or wait	1	6D594BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1CC.tmp.xml	success or wait	1	6D594BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCEC8.tmp.csv	success or wait	1	6D594BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD62C.tmp.txt	success or wait	1	6D594BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 00 00 59 58 07 60 21 05 06 00 00 00 00 00	MDMP..... .....YX.`!.....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	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 d4 37 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 64 08 00 00 4a 58 07 60 01 00 00 00 04 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.......7.... ..GenuineIntelW...........T... ....d...JX.`................. ....0................. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	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 7f 02 00 00 00 01 00 00 ff ff 00 00 9f 29 f4 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b b7 13 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 a4 ed e7 21 80 cb d4 1c fc ed e7 21 ff ff ff f9 00 00 00 00 80 cb d4 1c b4 ed e7 21 a3 79 09 1f 23 00 00 00 46 02 01 00 7c eb e7 21 2b 00 00 00 7f 02 00 01 00 00 00 00 9f 29 f4 72 00 00 00 00 00 00 00 00 00 00 00 00 00 80 1f 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....).r................ ....@..............+...S...+. ..+......!.......!............ ...!.y..#...F...|..!+......... ...).r........................	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	168	64 05 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 a3 79 09 1f 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 78 59 00 00	d........................y.... ....xY..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	20	60 03 00 00 00 10 b7 70 00 00 00 00 40 d7 07 00 0b e0 00 00	`......p....@.......	success or wait	864	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	513856	cc 3b fa 72 98 c3 6b 01 00 00 00 00 11 08 00 00 7f 00 00 00 00 00 00 00 80 a8 6b 01 00 00 00 26 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 00 00 00 c0 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 21 00 00 c0 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 10 00 00 c0 01 00 00 00 00 00 00 00 05 00 00 00 00 10 c9 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 15 d9 b7 70 b5 07 b8 70 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 18 00 00 c0 00 00 00 00 ec 3f bc 70 64 03 00 00 39 00 00 00 24 83 b7 70 00 00 00 00 60 28 bc 70 7e 01 00 00 1b 00 00	.;.r..k...................k... .&............................ ....!..... ....q.............. ....p...p ....?.pd...9...$..p ....`(.p~......	success or wait	863	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	524288	cc 3b fa 72 70 54 6b 01 00 00 00 00 11 08 00 00 7f 00 00 00 00 00 00 00 a0 ae 6b 01 00 00 00 26 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 00 00 00 c0 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 21 00 00 c0 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 10 00 00 c0 02 00 00 00 00 00 00 00 05 00 00 00 00 10 c9 71 00 10 93 73 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 b5 57 0d 71 a1 98 0d 71 b9 57 0d 71 a5 98 0d 71 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 d0 07 00 02 18 00 00 c0 00 00 00 00 d8 f8 1b 71 d2 08 00 00 c0 00 00 00 2c 07 0c 71 00 00 00 00 f4 c8 1b 71 a6 02 00 00 3e 00 00	.;.rpTk...................k... .&............................ ....!..... ....q...s.......... ....W.q...q .W.q...q...................... ....q........,..q ....q....>..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	12	55 c9 9f 00 4c 92 a0 00 95 92 a0 00	U...L.......	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	4	17 00 00 00	....	success or wait	23	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	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 7f 02 00 00 00 01 00 00 ff ff 00 00 ee a5 f7 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 ff 3f 00 00 00 00 00 00 00 80 ff 3f 00 00 00 00 00 00 00 80 ff 3f 00 00 00 00 00 00 00 a0 02 40 00 00 00 00 00 00 00 80 fd 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 e4 d6 d8 1c e0 ab d3 1c 08 31 cf 1c 00 00 00 00 00 00 00 00 00 00 00 00 c0 d0 2f 01 9c 2b 00 75 23 00 00 00 16 02 20 00 30 d0 2f 01 2b 00 00 00 7f 02 00 01 00 00 00 00 ee a5 f7 72 00 00 00 00 00 00 00 00 00 00 00 00 a0 1f 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	?............................ ....r................ ....?.... .....?.........?.........@.... .....?.............+...S...+. ..+............1.............. ../..+.u#..... .0./.+......... .....r........................	success or wait	23	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	48	84 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 b0 00 01 00 00 00 00 00 60 e1 0a 22 00 00 00 00 a0 1e 00 00 f9 eb 57 00 cc 02 00 00 cc 99 00 00	....`..".. ....W.........	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	4	5b 00 00 00	[...	success or wait	91	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	150	90 00 00 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 68 00 61 00 72 00 64 00 7a 00 5c 00 44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 5c 00 50 00 4f 00 20 00 32 00 30 00 31 00 30 00 30 00 32 00 39 00 5f 00 70 00 64 00 66 00 20 00 20 00 20 00 20 00 51 00 75 00 6f 00 74 00 61 00 74 00 69 00 6f 00 6e 00 20 00 20 00 66 00 72 00 6f 00 6d 00 20 00 41 00 6c 00 69 00 62 00 61 00 62 00 61 00 20 00 41 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	....C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.D.e.s.k.t.o.p.\.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.n. . .f.r.o.m. .A.l.i.b.a.b.a. .A.l.e...e.x.e...	success or wait	91	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	64	3a 00 00 00 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 53 00 79 00 73 00 74 00 65 00 6d 00 33 00 32 00 5c 00 6e 00 74 00 64 00 6c 00 6c 00 2e 00 64 00 6c 00 6c 00 00 00	:...C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.n.t.d.l.l...d.l.l...	success or wait	90	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	120	00 00 3a 70 00 00 00 00 00 d0 08 00 5a ea 08 00 d8 f6 7b 5a 9e 58 00 00 bd 04 ef fe 00 00 01 00 00 00 08 00 da 22 27 c6 00 00 08 00 da 22 27 c6 3f 00 00 00 0a 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 56 00 00 00 b1 a9 00 00 00 00 00 00 00 00 00 00 40 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..:p.....Z.....{Z.X.....'".....'".?.....V.....@.....	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	28	16 00 00 00 63 00 75 00 6c 00 74 00 75 00 72 00 65 00 2e 00 64 00 6c 00 6c 00 00 00	....c.u.l.t.u.r.e...d.l.l...	success or wait	2	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	1516	00 00 97 6d 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 3c 59 00 00 50 03 00 00 01 00 00 00 10 00 00 00 48 00 00 00 40 03 00 00 64 08 00 00 cc 02 00 00 00 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 24 00 00 00 78 00 00 00 40 01 00 00 b8 01 00 00 20 00 00 00 d8 01 00 00 24 01 00 00 00 03 00 00 38 00 00 00 38 03 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 01 05 00 00 00 00 00 00 05 15 00 00 00 cf 06 ad e5 49 85 b1 7e bc d2 94 f1 ea 03 00 00 00 00 00 00 0e 00 00 00 74 00 00 00 07 00 00 00 90 00 00 00 07 00 00 00 9c 00 00 00 07 00 00 00 a8 00 00 00 0f 00 00 00 b8 00 00 00 07 00 00 00 c8 00 00 00 07 00 00 00 d4 00 00 00 07 00 00 00 e0 00 00 00 07 00 00 00 ec 00 00 00 07 00 00 00 f8 00 00 00 07 00 00 00 04 01 00 00 07 00 00 c0 18 01 00	...m.....m.<Y..P.....H...@...d.....H...P...$...x...@..... .....$.....8...8.....l..~.....t.....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD288.tmp.mdmp	unknown	120	03 00 00 00 54 04 00 00 fc 06 00 00 04 00 00 00 68 26 00 00 5c 0b 00 00 0e 00 00 00 3c 00 00 00 c4 31 00 00 13 00 00 00 50 03 00 00 00 32 00 00 05 00 00 00 04 36 00 00 07 aa 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 15 00 00 00 ec 01 00 00 50 35 00 00 16 00 00 00 98 00 00 00 3c 37 00 00	....T.....h&..\.....<....1.....P....2.....6.....T.....8.....T.....P5.....<7..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.4.8.<./.P.i.d.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	144	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 4f 00 20 00 32 00 30 00 31 00 30 00 30 00 32 00 39 00 5f 00 70 00 64 00 66 00 20 00 20 00 20 00 20 00 51 00 75 00 6f 00 74 00 61 00 74 00 69 00 6f 00 6e 00 20 00 20 00 66 00 72 00 6f 00 6d 00 20 00 41 00 6c 00 69 00 62 00 61 00 62 00 61 00 20 00 41 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . .Q.u.o.t.a.t.i.o.n. . .f.r.o.m. . A.l.i.b.a.b.a. .A.l.e...e.x.e. <./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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.>.0.0.0.0.0.0.0.0.0.0. <./.C.m. d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 37 00 34 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.6.7.4.3. <./.U.p.t.i.m.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 36 00 37 00 36 00 39 00 30 00 30 00 38 00 36 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.>.6.7.6.9.0.0.8.6.4. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 36 00 37 00 31 00 35 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.6.7. 1.5.9.2.4.4.8.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	78	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 32 00 34 00 33 00 38 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.2.4.3.8.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 32 00 36 00 32 00 34 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.5.2.6.2.4.3.8.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 32 00 36 00 32 00 34 00 33 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.4.5.2.6.2.4.3.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 34 00 36 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.4.6.4.4.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 34 00 31 00 35 00 31 00 32 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.>.4.1.5.1.2.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	128	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 31 00 31 00 34 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.1.1.4.8.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	112	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 31 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.1.1.2.0.8.<./.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	80	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 30 00 33 00 32 00 30 00 30 00 30 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.>.4.4.0.3.2.0.0.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 31 00 30 00 31 00 36 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.4.4.1.0.1.6.3.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 30 00 33 00 32 00 30 00 30 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.>.4.4.0.3.2.0.0.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 36 00 34 00 33 00 33 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.3.6.4.3.3.6.<./.U.p.t.i.m.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4..g.u.e.s.t.=.".0.".h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 34 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.8.4.8.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 37 00 38 00 37 00 39 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.>.1.0.4.7.8.7.9.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 30 00 32 00 33 00 33 00 32 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.>.1.0.0.2.3.3.2.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 33 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.1.3.4.7.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 39 00 39 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.9.9.7.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.7.7.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.4.0.0.<./.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 39 00 37 00 30 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.7.0.4.1.9.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 39 00 32 00 39 00 35 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.9.2.9.5.3.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 39 00 37 00 30 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.7.0.4.1.9.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	148	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 50 00 4f 00 20 00 32 00 30 00 31 00 30 00 30 00 32 00 39 00 5f 00 70 00 64 00 66 00 20 00 20 00 20 00 20 00 51 00 75 00 6f 00 74 00 61 00 74 00 69 00 6f 00 6e 00 20 00 20 00 66 00 72 00 6f 00 6d 00 20 00 41 00 6c 00 69 00 62 00 61 00 62 00 61 00 20 00 41 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.P.O. .2.0.1.0.0.2.9._.p.d.f. . . . . Q.u.o.t.a.t.i.o.n. . .f.r.o.m. .A.l.i.b.a.b.a. .A.l.e...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 67 00 66 00 69 00 67 00 77 00 62 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.>.g.f.i.g.w.b.,. .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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 67 00 66 00 69 00 67 00 77 00 62 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.>.g.f.i.g.w.b.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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 35 00 32 00 39 00 35 00 35 00 36 00 34 00 32 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.>.1.5.5.2.9.5.5.6.4.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 31 00 39 00 54 00 32 00 32 00 3a 00 30 00 38 00 3a 00 32 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.1.9.T.2.2.:.0.8.:.2.7.Z.".>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 34 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 37 00 38 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 37 00 38 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.7.". .P.I.D.=.".2.1.4.8.". .U.p.t.i.m.e.M.S.=.".1.0.7.8.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.0.7.8.1.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 36 00 63 00 63 00 61 00 31 00 32 00 34 00 2d 00 61 00 35 00 62 00 63 00 2d 00 34 00 65 00 33 00 39 00 2d 00 62 00 63 00 65 00 66 00 2d 00 34 00 61 00 66 00 35 00 35 00 65 00 30 00 38 00 37 00 66 00 37 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.6.c.c.a.1.2.4.-.a.5.b.c.-.4.e.3.9.-.b.c.e.f.-.4.a.f.5.5.e.0.8.7.f.7.c.<./.G.u.i.d.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 31 00 39 00 54 00 32 00 32 00 3a 00 30 00 38 00 3a 00 32 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.1.9.T.2.2.:.0.8.:.2.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0D1.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	6D59497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1CC.tmp.xml	unknown	4777	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	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO 2010029_pdf _72613674f79bb87c1b11e7d393fe053666d79f1_6467c67c_1726352a\Report.wer	unknown	2	ff fe	..	success or wait	1	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO 2010029_pdf _72613674f79bb87c1b11e7d393fe053666d79f1_6467c67c_1726352a\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	221	6D59497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO 2010029_pdf _72613674f79bb87c1b11e7d393fe053666d79f1_6467c67c_1726352a\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 38 00 38 00 38 00 39 00 34 00 36 00 31 00 38 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.8.8.8.9.4.6.1.8.3.	success or wait	1	6D59497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{762d18d8-6432-fa3e-76aa-bc08f166954a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5B36BF	unknown
\REGISTRY\A\{762d18d8-6432-fa3e-76aa-bc08f166954a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5B36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D5B1FB2	RegCreateKeyExW
\REGISTRY\A\{762d18d8-6432-fa3e-76aa-bc08f166954a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5943D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 A3 79 09 1F 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D5B1FE8	RegSetValueExW

Analysis Process: WindowsUpdate.exe PID: 4848 Parent PID: 3388

General

Start time:	14:08:30
Start date:	19/01/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0xed0000
File size:	1074688 bytes
MD5 hash:	EB59D99961C7636B4872E389DA03CBC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000002.308445225.000000001EE00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000002.305904316.000000001C5F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.305904316.000000001C5F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.305904316.000000001C5F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.305904316.000000001C5F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000002.305904316.000000001C5F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000002.308219748.000000001DBD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.308219748.000000001DBD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.308219748.000000001DBD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.308219748.000000001DBD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000002.308219748.000000001DBD1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000002.300925836.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.300925836.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.300925836.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.300925836.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000002.300925836.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000008.00000002.305233571.000000001AD92000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.305233571.000000001AD92000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.305233571.000000001AD92000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.305233571.000000001AD92000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000008.00000002.305233571.000000001AD92000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	unknown	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1AEB0163	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1AEB0163	ReadFile

Analysis Process: WindowsUpdate.exe PID: 6328 Parent PID: 3388

General

Start time:	14:08:39
Start date:	19/01/2021
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\WindowsUpdate.exe'
Imagebase:	0xed0000
File size:	1074688 bytes
MD5 hash:	EB59D99961C7636B4872E389DA03CBC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.312787394.000000001EE40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.312583133.000000001DCB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.312583133.000000001DCB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.312583133.000000001DCB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.312583133.000000001DCB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.312583133.000000001DCB1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.301969493.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.301969493.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.301969493.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.301969493.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.301969493.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.312957269.000000001EED2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.312957269.000000001EED2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.312957269.000000001EED2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.312957269.000000001EED2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.312957269.000000001EED2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.309857450.000000001C5F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.309857450.000000001C5F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.309857450.000000001C5F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.309857450.000000001C5F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.309857450.000000001C5F0000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1EFB0163	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1EFB0163	ReadFile

Disassembly

Code Analysis