ID: 829699
Sample Name:
ChromeFIX_errorMEM.exe
Cookbook: default.jbs
Time: 00:26:07
Date: 19/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report ChromeFIX_errorMEM.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: RedLine 4
Yara Signatures 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 16
Public IPs 16
General Information 16
Warnings 17
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 18
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441\Report.wer
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp 1818
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp.xml 19
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log 19
C:\Windows\appcompat\Programs\Amcache.hve 19
C:\Windows\appcompat\Programs\Amcache.hve.LOG1 20
Static File Info 20
General 20
File Icon 20
Static PE Info 20
General 20
Entrypoint Preview 21
Rich Headers 22
Data Directories 22
Sections 22
Resources 23
Imports 23
Possible Origin 23
Network Behavior 23
Snort IDS Alerts 23
TCP Packets 24
Statistics 25
Behavior 25
System Behavior 26
Analysis Process: ChromeFIX_errorMEM.exePID: 5764, Parent PID: 3452 26
General 26
File Activities 26
Analysis Process: conhost.exePID: 5772, Parent PID: 5764 26
General 26

Analysis Process: AppLaunch.exePID: 5828, Parent PID: 5764 27
General 27
File Activities 27
File Created 27
File Written 27
File Read 28
Analysis Process: WerFault.exePID: 5884, Parent PID: 5764 30
General 31
File Activities 31
File Created 31
File Deleted 31
File Written 31
Registry Activities 54
Key Created 54
Key Value Created 54
Disassembly 55

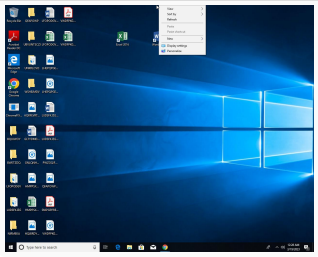
Windows Analysis Report

ChromeFIX_errorMEM.exe

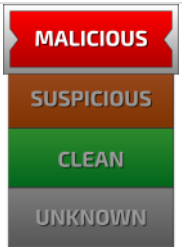
Overview

General Information

Sample Name:	ChromeFIX_errorMEM.exe
Analysis ID:	829699
MD5:	74b6b35627f64..
SHA1:	a9282e204443...
SHA256:	51921d13908b...
Tags:	exe
Infos:	



Detection



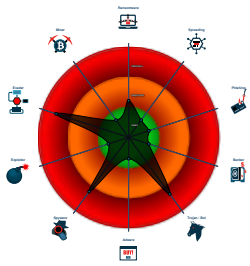
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle...
- Machine Learning detection for sam...
- Allocates memory in foreign process...
- Injects a PE file into a foreign proce...
- Queries sensitive video device infor...
- Contains functionality to inject code...
- Queries sensitive disk information (v...

Classification



Process Tree

- **System is w10x64**
- ChromeFIX_errorMEM.exe (PID: 5764 cmdline: C:\Users\user\Desktop\ChromeFIX_errorMEM.exe MD5: 74B6B35627F6453D787F1C7EA3B9EC33)
  - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 5828 cmdline: C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
  - WerFault.exe (PID: 5884 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5764 -s 132 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
RedLine Stealer	RedLine Stealer is a malware available on underground forums for sale apparently as standalone ($100/$150 depending on the version) or also on a subscription basis ($100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.	No Attribution	**http://** https://asec.ahnlab.com/en/30445/https://asec.ahnlab.com/en/35981/https://asec.ahnlab.com/ko/25837/https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.htmlhttps://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: RedLine

Copyright Joe Security LLC 2023

```
{
  "C2 url": [
    "135.181.173.163:4323"
  ],
  "Authorization Header": "a909e2aaecf96137978fea4f86400b9b"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.304460782.0000000000402000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.247722749.0000000000FE0000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.240337295.0000000000F82000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: AppLaunch.exe PID: 5828	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: AppLaunch.exe PID: 5828	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.2.AppLaunch.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a434:$pat14: , CommandLine: • 0x134a2:$v2_1: ListOfProcesses • 0x13281:$v4_3: base64str • 0x13e05:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12814:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.3.ChromeFIX_errorMEM.exe.f80000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.ChromeFIX_errorMEM.exe.f80000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a434:$pat14: , CommandLine: • 0x134a2:$v2_1: ListOfProcesses • 0x13281:$v4_3: base64str • 0x13e05:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12814:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.ChromeFIX_errorMEM.exe.fd0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2023

Snort Signatures

ET TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 135.181.173.163	
Timestamp:	192.168.2.3135.181.173.1634968543232043233 03/19/23-00:27:09.983730
SID:	2043233
Source Port:	49685
Destination Port:	4323
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 135.181.173.163 - Destination IP: 192.168.2.3	
Timestamp:	135.181.173.163192.168.2.34323496852043234 03/19/23-00:27:12.062612
SID:	2043234
Source Port:	4323
Destination Port:	49685
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 135.181.173.163	
Timestamp:	192.168.2.3135.181.173.1634968543232043231 03/19/23-00:27:21.986883
SID:	2043231
Source Port:	49685
Destination Port:	4323
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

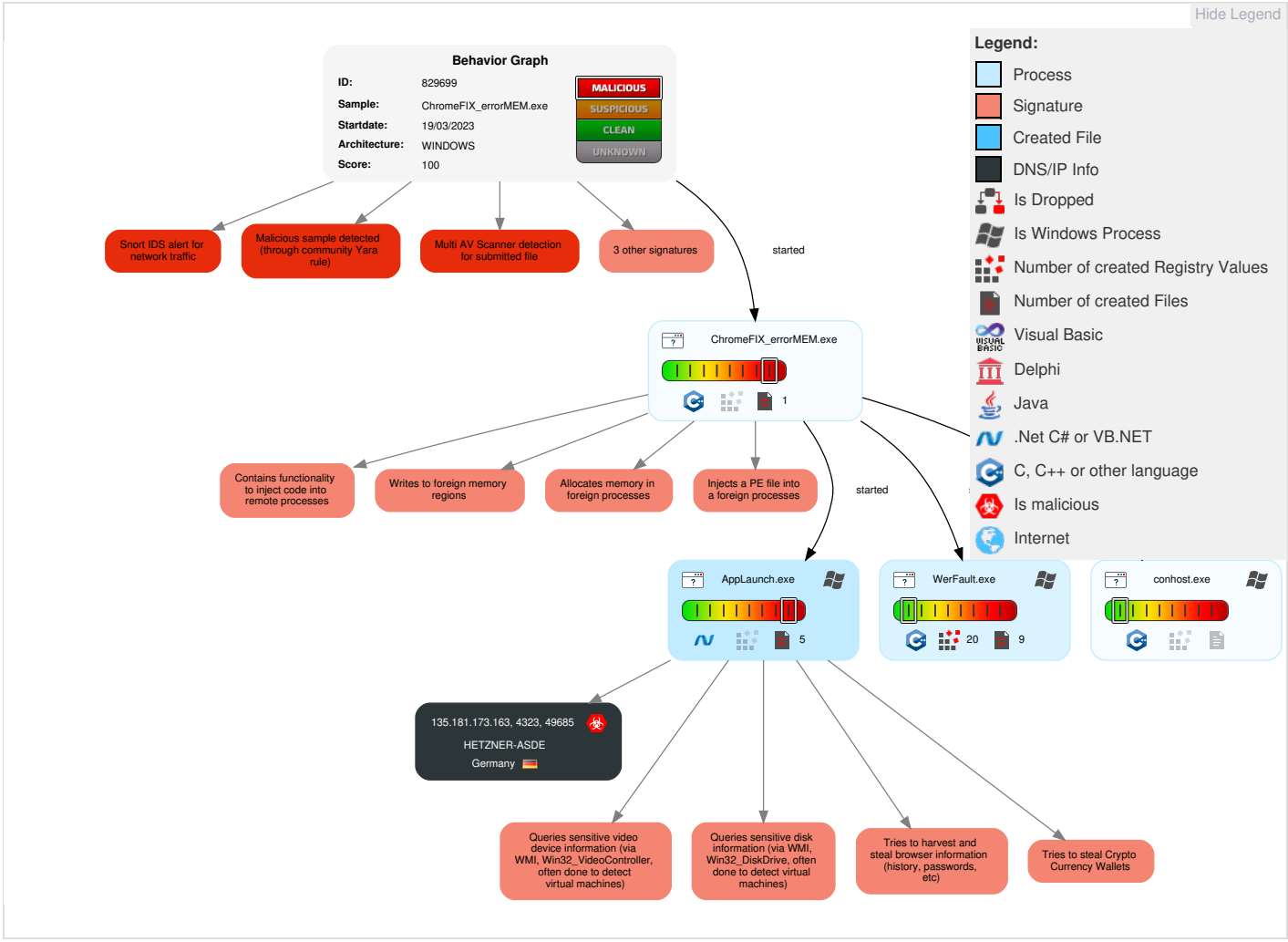
Remote Access Functionality

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 1 Windows Management Instrumentation	Path Interception	4 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 5 1 Security Software Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 1 Process Injection	NTDS	2 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

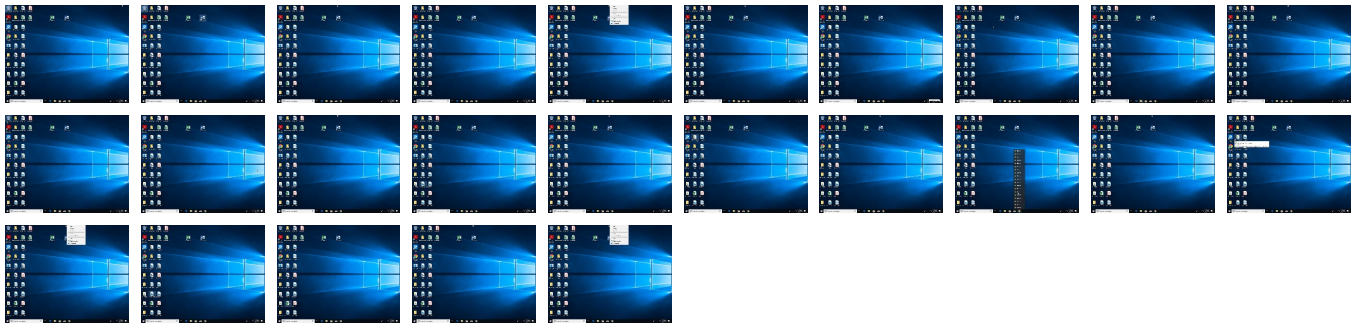
Behavior Graph



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
ChromeFIX_errorMEM.exe	38%	ReversingLabs	Win32.Trojan.CryptErX	
ChromeFIX_errorMEM.exe	49%	Virustotal		Browse
ChromeFIX_errorMEM.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
0.3.ChromeFIX_errorMEM.exe.f80000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2023

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://ns.ado/1.0/s	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17Response	0%	URL Reputation	safe	
135.181.173.163:4323	0%	Avira URL Cloud	safe	
135.181.173.163:4323	4%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
135.181.173.163:4323	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultP	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	AppLaunch.exe, 00000002.00000002.3107298 21.0000000007FCC000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.310729821.000000000838E00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.310729821.000 00000080C8000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.310729821.00000000080E5000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.305735344 .0000000007499000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.310729821.0000000007FE9000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.30573 5344.0000000007148000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.310729821.0000000008371 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.305735344.0 000000007409000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.305735344.000000000702B000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3057353 44.00000000071D5000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.310729821.000000000804A00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.310729821.000 0000008067000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.305735344.00000000070BB000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	AppLaunch.exe, 00000002.00000002.3107298 21.0000000008067000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.305735344.00000000070BB00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FC3000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.305735344.0000000006F2100 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.305735344.000 0000006FAF000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id8	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FC3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	ChromeFIX_errorMEM.exe, ChromeFIX_errorMEM.exe, 00000000.00000002.247722749.0000000000FE0000.00000004.00000001.01000000.00000003.sdmp, ChromeFIX_errorMEM.exe, 00000000.00000003.240337295.0000000000F82000.00000040.00001000.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.305735344.0000000006FC3000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.304460782.0000000000402000.00000020.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high

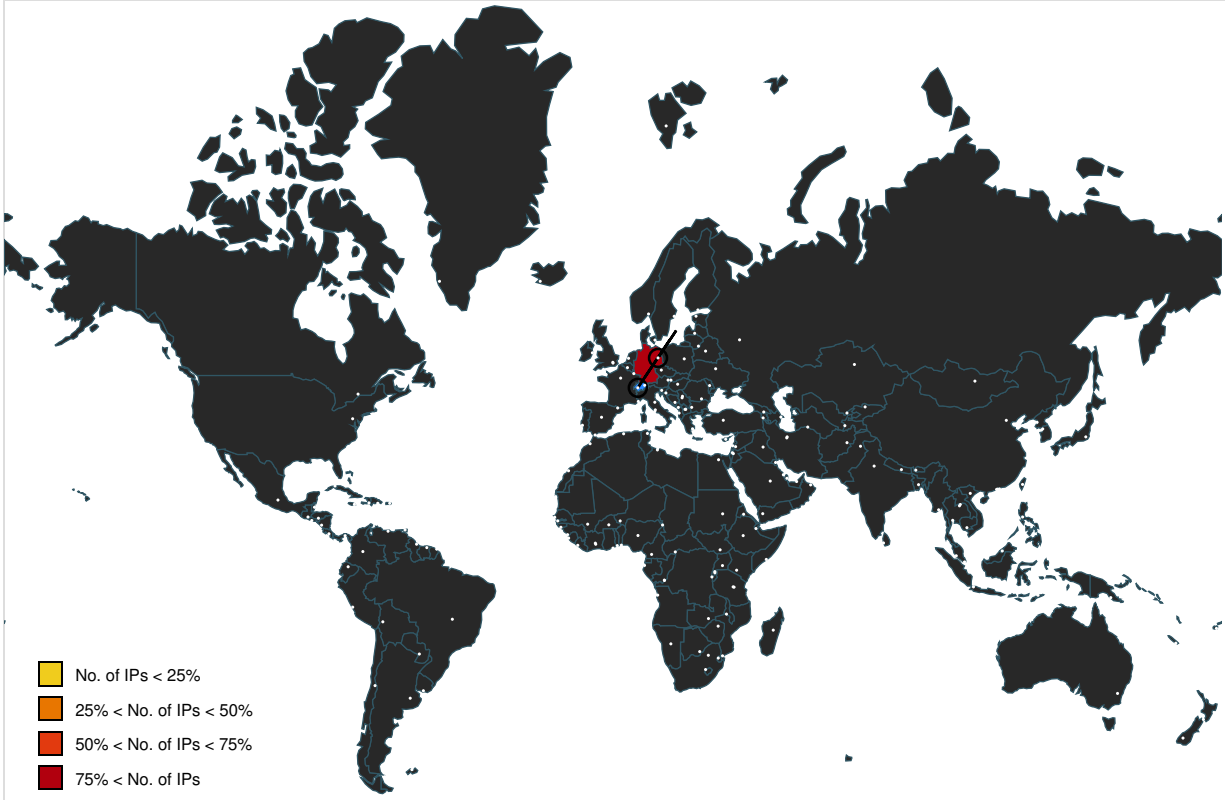
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AppLaunch.exe, 00000002.00000002.3107298 21.0000000008067000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.305735344.00000000070BB00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	AppLaunch.exe, 00000002.00000002.3107298 21.0000000007FCC000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.310729821.000000000838E00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.310729821.000 00000080C8000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.310729821.00000000080E5000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.305735344 .0000000007499000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.310729821.0000000007FE9000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.30573 5344.0000000007148000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.310729821.0000000008371 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.305735344.0 000000007409000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.305735344.000000000702B000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3057353 44.00000000071D5000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.310729821.000000000804A00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.310729821.000 0000008067000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.305735344.00000000070BB000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	AppLaunch.exe, 00000002.00000002.3107298 21.0000000007FCC000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.310729821.000000000838E00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.310729821.000 00000080C8000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.310729821.00000000080E5000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000002.305735344 .0000000007499000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000002.310729821.0000000007FE9000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.30573 5344.0000000007148000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000002.310729821.0000000008371 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.305735344.0 000000007409000.00000004.00000800.000200 00.00000000.sdmp, AppLaunch.exe, 0000000 2.00000002.305735344.000000000702B000.00 000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.3057353 44.00000000071D5000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.310729821.000000000804A00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.310729821.000 0000008067000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.305735344.00000000070BB000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://ns.ado/1.0/s	AppLaunch.exe, 00000002.00000002.3056246 77.00000000054C6000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wscoor	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006FAF000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17Response	AppLaunch.exe, 00000002.00000002.3057353 44.0000000006F21000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
135.181.173.163	unknown	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829699
Start date and time:	2023-03-19 00:26:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0

Copyright Joe Security LLC 2023

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
Sample file name:	ChromeFIX_errorMEM.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/7@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 90.7% (good quality ratio 87%) • Quality average: 82.8% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22
- Excluded domains from analysis (whitelisted): fs.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target AppLaunch.exe, PID 5828 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:27:01	API Interceptor	1x Sleep call for process: WerFault.exe modified
00:27:26	API Interceptor	15x Sleep call for process: AppLaunch.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8431639159677459
Encrypted:	false
SSDEEP:	96:aFeMHFau7TeecwtoI7Rj6tpXIQcQvc6QcEDMcw3Db+HbHg/8BRTf3OFL9iVffYEs:QMu7fwHBUZMXYjJSq/u7sWS274ItJz
MD5:	932664183AA0A32C0E1B63E46AA0FFDA
SHA1:	DFD33ECC6A7B5717CDCE2947D4BC682678A35BB7
SHA-256:	731413517DFB42E2D12A6D01BA9A60A14F85A9916A1CB27DD8E97C9CEB9BD63C
SHA-512:	F47A833A117DE80992809E0307A34C0FD5F63D2B0261ECB2F65EC6DB52C5B905776DE066B8AB66C21E71B33030438CADBE994331063941E2DB9C465659D3942
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.3.6.8.4.4.1.9.1.8.4.0.5.8.9.....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.=.1.3.3.2.3.6.8.4.4.1.9.7.3.0.9.4.9.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.f.2.5.d.5.3.a.-.a.9.1.c.-.4.9.8.6.-.a.a.1.4.-.f.0.a.2.6.e.9.a.1.a.3.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.1.5.5.1.d.e.3.-.1.7.3.c.-.4.8.a.3.-.8.0.f.5.-.d.e.e.0.3.0.7.c.2.6.0.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.C.h.r.o.m.e.F.I.X._.e.r.r.o.r.M.E.M...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.8.4.-.0.0.0.1.-.0.0.1.f.-.2.0.7.e.-.d.d.2.f.3.4.5.a.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.2.0.4.c.f.7.6.6.2.8.a.2.9.3.7.7.5.9.c.3.b.1.8.0.8.0.e.c.d.3.e.0.0.0.0.1.a.0.8.!.0.0.0.0.a.9.2.8.2.e.2.0.4.4.4.3.f.e.d.6.e.0.b.e.2.8.e.8.e.2.d.f.e.7.c.9.2.7.7.0.6.4.2.8.!.C.h.r.o.m.e.F.I.X._.e.r.r.o.r.M.E.M...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Mar 19 07:26:59 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	45376
Entropy (8bit):	1.8124432683259049
Encrypted:	false
SSDEEP:	192:PYNhZ7wO64/9+6J1QxS7obbS4Eu83YQO:o6y+gCJ/Eu8I5
MD5:	41DB3C3E47377B047B1DE1E5FFD5C8BC
SHA1:	88191D097E0AAEA3EDA8E129CD653EC4C576FFC8
SHA-256:	EE0194B9F7BDF480A5581080E7E50708F4936A3AA4E5D9FF89E6699FFD08CBD4
SHA-512:	39892083ACD433A09CFC584E5B28C9B9A23AFB0A802684A66610AC4E07C559DDBEC1DCCF48A5B87FF6171CF188E7169F9C033D4391C41A8DE6FF9046DA6D827
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....C..d.....)..... .....T.....8.....T.....@.....U.....B.....h.....GenuineIntelW.....T.....A..d.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8434
Entropy (8bit):	3.700284113308964
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiK2646YqASUOMvgmfaxmSxCpr/89blLsf+U3m:RrlsNir646YtSUdgmfrShlQfU
MD5:	63F6B02D4E232F69FC8F56115D6D36E7
SHA1:	8AC18D6573CFE28C82C1DCE437D9C86AC1C7B551
SHA-256:	B32C3C77A4D4EFC30FA5695A2AD1C04D0C7D3675BAA9132C433075F3C753E540

SHA-512:	5064063B7DE8EA497A026C614B521C99CFA64811CEE8A909D8031E27998C6F966006AEF4903722ECE476877F29A3DA823FB77274429DB96E38CDFBF9EFB19CDE
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.7.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4756
Entropy (8bit):	4.505325155750122
Encrypted:	false
SSDEEP:	48:cvIwSD8zsrJgtWI9/iVSWgc8sqYjf8fm8M4JA2gGMF6+q8vLgGYOvSWdutltfd:uITfFliVzgrsqYoJpDKnYAUefd
MD5:	8E71765A94A747E842E3E511ACA1C481
SHA1:	1BCF6F023AEDD246F13084E27DECF3891F65C13D
SHA-256:	5C5939271ACBBAF82A589CCF7307A8C541F1449F556EA5BFE2C37FE2BA36CD29
SHA-512:	B0B682AB135A1272D22A308F847CCB0E5B607B883DAEFAE7B3184EB2C172BE7243FC01E46EE0212DFBDC0D09C8A2653455BF9DCCB8B196E8C90B603DE44DBFCF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1959397" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2752
Entropy (8bit):	5.335270411216887
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHlmHKx1qHjq:iqXeqm00YqhQnouOqLqdqNq2qzcGtIx4
MD5:	325ECAAB191D9F741B127964E978A5D3
SHA1:	B5E61B16E9399D102A00613323001CD69AC3E97A
SHA-256:	38B47B7B5BA6D77CED448D8396426AC9B6C722A12F61793D3FD79E3AD1615123
SHA-512:	D5017FC87DA83B8A1B336B3FBF779CB5040F3C0AD4FD4D9D661E7D953C816648D09D24A46B8C3A75F65CE717E237E350F0489EC3491844D791D4AFE2E8368BB4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.288770781817703
Encrypted:	false
SSDEEP:	12288:XcJvy5zN1sUbP5nASQw0IQYVA17eAVAG1HxbZC30pr1ci+fDDLnbwOzb:Wvy5zN1sUbP5nA6yWX
MD5:	D94238BC69165D83EFA7BFAF027528CE

SHA1:	84D7B17EE2B4E6171B8D500B0CA61531DF6A5DE6
SHA-256:	095DDD91051AF1AD2181EBF7C5874B59944E777880FBC8F10BAB2321AF26C14E
SHA-512:	2CECCA35BD98A5F35FF4D206D073BA02E618F10E94A0C3C47171FE0AD42743B75D288C372066621FF73945D6B453E092CE51CE852D680CC789FE086AC5D2B6 2
Malicious:	false
Preview:	regfj...j...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.N.04Z..... ....w.m..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.8172451480315845
Encrypted:	false
SSDEEP:	768:qCeRftx1sJ4JnHFAJfXqp+pkkqIDSC9OeMYUC5Wf:++im6i
MD5:	7C21FF446BEB27DAE44DA9E1C7DB0C2E
SHA1:	53A45C582CD93E62AB52026AAEECE59C72CA8F6C
SHA-256:	AD4F07B60AA90C2EB8809688E529F537603C98B591E545298CEFB57CAD61EE68
SHA-512:	4583C8355106D5050974D3E6B4F982910F5800DB71F81EF4DB94C2F6D1AFB6405F14F0962B2BF33D0C9DFD25CBDEDF51DE3950A0B5005B4FC203F15E5C1E479
Malicious:	false
Preview:	regfi...i...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.N.04Z..... ....w.mHvLE.n.....i.....8.t.....0.....0..hbin.....p.\.,.....nk,.:..04Z..... .....&...{ad79c032-a2ea-f756-e377- 72fb9332c3ae}.....nk .:..04Z..... ....Z.....Root.....lf.....Root....nk .:..04Z.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.228703310847611
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ChromeFIX_errorMEM.exe
File size:	253952
MD5:	74b6b35627f6453d787f1c7ea3b9ec33
SHA1:	a9282e204443fed6e0be28e8e2dfe7c927706428
SHA256:	51921d13908bd84b1c8fbdd77e6e29d4359ce0fc40857f6f0ad15b1b6ee74730
SHA512:	da3758d999b7a593987aa8e9d708b0b3215a442dc1f3470a81f3ddc221b7875d6c9ecb1c53fce5e7ee795a20e7267d21e8fac804089bb1b65e838c0ed9530996
SSDEEP:	3072:W1jGFFPBsryKxPUBnIZ/C9FUYHwKLLgQmsbVVTjC3r7wcLl2byii5DzrIlu:ug3iPUZIAFUYHDPaQVXC3xR2/iNo
TLSH:	9B441813311F3E60E1FA69B8889DF3865516E3710A6DDB5D73AB0E2E4D09DC39920B36
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c-.H.C.H.C.H.C.VP.. [.C.VP....C.VP..m.C.o.8.L.C.....K.C.H.B...C.Az..I.C.VP..I.C.Az..I.C.RichH.C.....PE..L...jp.d.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40370b
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6415706A [Sat Mar 18 08:03:54 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	df35d969e1568731b4c070bee6bd7122

Entrypoint Preview

Instruction
call 00007F01BC9D1301h
jmp 00007F01BC9CECF9h
mov edi, edi
push esi
push 00000001h
push 0043C3E4h
mov esi, ecx
call 00007F01BC9D1381h
mov dword ptr [esi], 0040D8D4h
mov eax, esi
pop esi
ret
mov dword ptr [ecx], 0040D8D4h
jmp 00007F01BC9D13E6h
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
mov dword ptr [esi], 0040D8D4h
call 00007F01BC9D13D3h
test byte ptr [ebp+08h], 00000001h
je 00007F01BC9CEE59h
push esi
call 00007F01BC9CFD1Dh
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F01BC9D1352h
mov dword ptr [esi], 0040D8D4h
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi

Instruction
push ebp
mov ebp, esp
sub esp, 0Ch
jmp 00007F01BC9CEE5Fh
push dword ptr [ebp+08h]
call 00007F01BC9D166Bh
pop ecx
test eax, eax
je 00007F01BC9CEE61h
push dword ptr [ebp+08h]
call 00007F01BC9D1585h
pop ecx
test eax, eax
je 00007F01BC9CEE38h
leave
ret
test byte ptr [0043D420h], 00000001h
mov esi, 0043D414h
jne 00007F01BC9CEE6Bh
or dword ptr [0043D420h], 01h
mov ecx, esi
call 00007F01BC9CEDA9h
push 0040C9BBh
call 00007F01BC9D14F2h
pop ecx
push esi
lea ecx, dword ptr [ebp-0Ch]
call 00007F01BC9DEDE2h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 SP1 build 30729 • [RES] VS2008 build 21022 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf5f4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3f000	0xd44	.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	0xd000	0x10c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb9cf	0xba00	False	0.5594758064516129	data	6.743605377395388	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x2c1a	0x2e00	False	0.45541779891304346	data	5.897601757940328	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x10000	0x2dffc	0x2d400	False	0.5448355490331491	data	7.176585474224499	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3e000	0x5c8	0x600	False	0.44921875	data	3.9110725913804987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3f000	0x1940	0x1a00	False	0.43704927884615385	data	4.306560145331581	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3e200	0x3c8	data	English	United States
RT_MANIFEST	0x3e0a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetNativeSystemInfo, IsValidCodePage, GetModuleHandleA, FreeConsole, MultiByteToWideChar, GetProcAddress, GetCommandLineA, SetUnhandledExceptionFilter, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetLastError, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, HeapFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapAlloc, RaiseException, GetCPInfo, GetACP, GetOEMCP, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, IsDebuggerPresent, LeaveCriticalSection, EnterCriticalSection, LoadLibraryA, InitializeCriticalSectionAndSpinCount, VirtualAlloc, HeapReAlloc, RtlUnwind, HeapSize, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA
USER32.dll	ShowScrollBar
COMDLG32.dll	GetSaveFileNameA, GetOpenFileNameA

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3135.181.173.163496854323204323303/19/23-00:27:09.983730	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49685	4323	192.168.2.3	135.181.173.163
135.181.173.163192.168.2.34323496852043234 03/19/23-00:27:12.062612	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	4323	49685	135.181.173.163	192.168.2.3
192.168.2.3135.181.173.163496854323204323103/19/23-00:27:21.986883	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49685	4323	192.168.2.3	135.181.173.163

TCP Packets

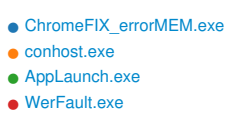
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 00:27:09.580728054 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:09.620574951 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:09.620807886 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:09.983730078 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:10.022506952 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:10.073775053 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:12.021528006 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:12.062612057 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:12.105101109 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:21.986882925 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.028717995 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.028784037 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.028834105 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.028870106 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.028879881 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.028928995 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.028963089 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.028975964 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.029021978 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.029045105 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.029067993 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.029112101 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.029135942 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.029179096 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.029259920 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.067349911 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.067409039 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.067455053 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.067471027 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.067502022 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.067550898 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.067560911 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:22.067599058 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:22.067647934 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.756911039 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.795286894 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.795412064 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.795428038 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.795505047 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.795744896 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.795902967 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.833750010 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.833802938 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.833991051 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.834032059 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.834178925 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.834249020 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.834317923 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.872215986 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.872273922 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.872312069 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.872431993 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.872531891 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.872695923 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.872868061 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.872890949 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.873018026 CET	49685	4323	192.168.2.3	135.181.173.163

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 00:27:27.873039007 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.873148918 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.873179913 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.873322010 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.873339891 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.873512983 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.873699903 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.873703003 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.873814106 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.874046087 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.874164104 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.911107063 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911156893 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911194086 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911226988 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911408901 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.911408901 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.911484003 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911611080 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.911679029 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911715031 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911822081 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.911822081 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.911865950 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.911940098 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.912010908 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.912112951 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.912363052 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.912436008 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.912502050 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.912569046 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.912797928 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.912961006 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.912981033 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.913053989 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.913086891 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.913158894 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.913357973 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.913427114 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.913539886 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.913635015 CET	49685	4323	192.168.2.3	135.181.173.163
Mar 19, 2023 00:27:27.913680077 CET	4323	49685	135.181.173.163	192.168.2.3
Mar 19, 2023 00:27:27.913739920 CET	49685	4323	192.168.2.3	135.181.173.163

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ChromeFIX_errorMEM.exe PID: **5764**, Parent PID: **3452**

General

Target ID:	0
Start time:	00:26:57
Start date:	19/03/2023
Path:	C:\Users\user\Desktop\ChromeFIX_errorMEM.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ChromeFIX_errorMEM.exe
Imagebase:	0xfd0000
File size:	253952 bytes
MD5 hash:	74B6B35627F6453D787F1C7EA3B9EC33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.247722749.0000000000FE0000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.240337295.0000000000F82000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5772**, Parent PID: **5764**

General

Target ID:	1
Start time:	00:26:57
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: AppLaunch.exe PID: **5828**, Parent PID: **5764**

General

Target ID:	2
Start time:	00:26:58
Start date:	19/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe
Imagebase:	0x40000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.304460782.0000000000402000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	0	2752	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Users\user\Desktop\LFOPODGVOH\LFOPODGVOH.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH\LFOPODGVOH.docx	unknown	1022	end of file	1	717E1B4F	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LFOPODGVOH\LFOPODGVOH.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH\HMPPSXQPQV.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH\HMPPSXQPQV.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH\HMPPSXQPQV.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG\LIJDSFKJZG.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG\LIJDSFKJZG.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG\LIJDSFKJZG.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG\VWDFPKGDUF.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG\VWDFPKGDUF.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG\VWDFPKGDUF.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\UNKRLCVOHV\UNKRLCVOHV.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\UNKRLCVOHV\UNKRLCVOHV.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\UNKRLCVOHV\UNKRLCVOHV.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\UNKRLCVOHV\LFOPODGVOH.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\UNKRLCVOHV\LFOPODGVOH.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\UNKRLCVOHV\LFOPODGVOH.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\GLTYDMDUST.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\GLTYDMDUST.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\GLTYDMDUST.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\HMPPSXQPQV.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\HMPPSXQPQV.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\HMPPSXQPQV.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LFOPODGVOH.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\VWDFPKGDUF.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\VWDFPKGDUF.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\VWDFPKGDUF.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH\LFOPODGVOH.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH\LFOPODGVOH.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH\LFOPODGVOH.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH\HMPPSXQPQV.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH\HMPPSXQPQV.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH\HMPPSXQPQV.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG\LIJDSFKJZG.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG\LIJDSFKJZG.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG\LIJDSFKJZG.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG\VWDFPKGDUF.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG\VWDFPKGDUF.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG\VWDFPKGDUF.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV\UNKRLCVOHV.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV\UNKRLCVOHV.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV\UNKRLCVOHV.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV\LFOPODGVOH.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV\LFOPODGVOH.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV\LFOPODGVOH.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LIJDSFKJZG.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\UNKRLCVOHV.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\UNKRLCVOHV.docx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\HMPPSXQPQV.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\HMPPSXQPQV.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\HMPPSXQPQV.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\LFOPODGVOH.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\VWDFPKGDUF.xlsx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\VWDFPKGDUF.xlsx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\VWDFPKGDUF.xlsx	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	13	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ Network\Cookies	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ Network\Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile

Analysis Process: WerFault.exe PID: **5884**, Parent PID: **5764**

General

Target ID:	4
Start time:	00:26:58
Start date:	19/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5764 -s 132
Imagebase:	0xf40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A5E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A5D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp.xml	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB00.tmp.csv	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB10.tmp.txt	success or wait	1	6A5D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 43 fd 16 64 fd 05 12 00 00 00 00 00	MDMP Cd	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	5992	6	00 00 00 00 00 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 68 17 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 16 00 00 41 fd 16 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBhGenuineIntelWTAd0 Pacific Standard TimePacific Daylight Time	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	6944	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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 0c 5d 08 fd 01 00 00 00 30 18 fd 02 00 00 fd 02 31 78 fd 00 00 00 00 00 fd 31 fd 00 0c 5d 08 fd 23 00 00 00 46 02 01 00 fd fd 5a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++]01x1]#FZ+	success or wait	1	6A5D497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 0c 5d 08 fd fd fd fd 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 0c 5d 08 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 20 1b 00 00	]]	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	10524	20	10 00 00 00 70 fd fd 00 00 00 00 00 fd 03 00 00 20 2a 00 00	p *	success or wait	16	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	10784	912	fd fd fd 77 fd 4c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 04 fd fd 00 fd fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd 00 70 61 00 00 70 61 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 70 61 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 6e fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 fd fd 00 00 00 00 00 00 00 00 00 48 6a fd 00 00 fd 60 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 01 01 01 01 00 00 01 01 78 fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww@w@wpapapanHj`x	success or wait	15	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	35400	2388	fd fd fd 77 fd 4c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 40 fd fd 00 0c fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd 00 fd 61 00 00 fd 61 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 61 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 6e fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 10 01 fd 00 00 00 00 00 00 00 00 00 48 6a fd 00 00 fd 60 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 01 01 01 01 00 00 01 01 54 fd 60 00 3c fd fd 00 fd 6e fd 00 44 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww@@w@waaanHj`T`<nD	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6A5D497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	7660	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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 31 78 fd 00 00 00 00 00 fd fd 5a 00 fd fd fd 77 23 00 00 00 12 02 00 00 40 fd 5a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++1xZw#@Z+	success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	1936	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 61 00 00 00 00 00 fd fd fd 00 00 00 00 00 54 09 00 00 48 fd 00 00 fd 02 00 00 50 26 00 00	aTHP&	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	1996	4	1f 00 00 00		success or wait	31	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	5998	50	2c 00 00 00 43 00 68 00 72 00 6f 00 6d 00 65 00 46 00 49 00 58 00 5f 00 65 00 72 00 72 00 6f 00 72 00 4d 00 45 00 4d 00 2e 00 65 00 78 00 65 00 00 00	,ChromeFIX_errorMEM.exe	success or wait	31	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	5240	752	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 08 1b 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 fd 5f 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 13 68 03 00 00 00 00 00 a0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1b 00 00 00 00 00 fd 69 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 0b fd 04 00 00 00 00	t`A!-aBB?#@AZbP_hi@	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	37788	7588	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB77.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 18 0d 00 00 fd 07 00 00 05 00 00 00 04 01 00 00 1c 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 15 00 00 40 fd 00 00 15 00 00 00 fd 01 00 00 fd 14 00 00 16 00 00 00 fd 00 00 00 fd 16 00 00	)T8T@	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5764</Pid>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1002	90	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 43 00 68 00 72 00 6f 00 6d 00 65 00 46 00 49 00 58 00 5f 00 65 00 72 00 72 00 6f 00 72 00 4d 00 45 00 4d 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	<ImageName>ChromeFIX_errorMEM.exe</ImageName>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1092	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1096	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1100	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1190	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1194	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1198	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2282</Uptime>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1240	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1244	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1248	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	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1330	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1334	2	09 00		success or wait	2	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1338	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	<IptEnabled>0</IptEnabled>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1390	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1394	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1398	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	<ProcessVmInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1442	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1446	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1452	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 33 00 37 00 33 00 34 00 35 00 32 00 38 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	<PeakVirtualSize>83734528</PeakVirtualSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1538	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1542	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1548	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 31 00 37 00 37 00 32 00 35 00 34 00 34 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	<VirtualSize>81772544</VirtualSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1618	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1622	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1628	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 38 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1828</PageFaultCount>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1712	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 38 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6881280</PeakWorkingSetSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1808	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1812	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1818	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 32 00 38 00 30 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6828032</WorkingSetSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1898	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1902	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	1908	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>154736</QuotaPeakPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2022	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2026	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2032	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 33 00 37 00 36 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	<QuotaPagedPoolUsage>153768</QuotaPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2130	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2134	2	09 00		success or wait	3	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2140	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<QuotaPeakNonPagedPoolUsage>20632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2264	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2268	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2274	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>20360</QuotaNonPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2382	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2386	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2392	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 38 00 37 00 35 00 35 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	<PagefileUsage>1687552</PagefileUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2478	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 32 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1892352</PeakPagefileUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2570	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2574	2	09 00		success or wait	3	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2580	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 38 00 37 00 35 00 35 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	<PrivateUsage>1687552</PrivateUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2652	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2656	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2660	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	</ProcessVmInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2706	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2710	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2714	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	<ParentProcess>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2744	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2748	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2754	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	<ProcessInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2794	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2798	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2806	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2836	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2840	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2848	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	<ImageName>explorer.exe</ImageName>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	2930	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	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3032	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 38 00 35 00 33 00 37 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4385375</Uptime>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3080	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3084	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3092	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	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3182	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	<IptEnabled>0</IptEnabled>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3246	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	<ProcessVmInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3304	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	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3408	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	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3496	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 36 00 30 00 34 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	<PageFaultCount>60497</PageFaultCount>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3572	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3576	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3586	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 32 00 33 00 38 00 39 00 39 00 39 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	<PeakWorkingSetSize>123899904</PeakWorkingSetSize>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3686	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3690	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3700	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 34 00 34 00 35 00 32 00 34 00 38 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	<WorkingSetSize>123445248</WorkingSetSize>	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3784	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3788	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3798	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11429 52</QuotaPeakPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3914	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3918	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	3928	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 37 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1107304</ QuotaPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4028	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4032	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4042	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 39 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>92 528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4166	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4170	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4180	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 38 00 33 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	<QuotaNonPagedPoolUsage>83912< /QuotaNonPagedPoolUsage>	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4288	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4292	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4302	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 34 00 37 00 30 00 30 00 35 00 36 00 39 00 36 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	<PagefileUsage>4700569</PagefileUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4380	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4384	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4394	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 34 00 38 00 32 00 37 00 31 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>48271360</PeakPagefileUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4488	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4492	2	09 00		success or wait	5	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4502	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 34 00 37 00 30 00 30 00 35 00 36 00 39 00 36 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	<PrivateUsage>4700569</PrivateUsage>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4576	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4580	2	09 00		success or wait	4	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4588	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	</ProcessVmInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4634	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4638	2	09 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4644	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	</ProcessInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4686	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4690	2	09 00		success or wait	2	6A5D497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4694	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	</ParentProcess>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4732	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	</ProcessInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4774	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4778	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4780	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	<ProblemSignatures>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4826	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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	<EventType>BEX</EventType>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4878	4	0d 00 0a 00		success or wait	9	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4882	2	09 00		success or wait	18	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	4886	94	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 43 00 68 00 72 00 6f 00 6d 00 65 00 46 00 49 00 58 00 5f 00 65 00 72 00 72 00 6f 00 72 00 4d 00 45 00 4d 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>ChromeFIX_errorMEM.exe</Parameter0>	success or wait	9	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5628	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5632	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5634	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	</ProblemSignatures>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5674	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5678	2	09 00		success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5680	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	<DynamicSignatures>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5718	4	0d 00 0a 00		success or wait	6	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5722	2	09 00		success or wait	12	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	5726	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6286	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	</DynamicSignatures>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6326	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6330	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6332	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	<SystemInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6370	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6374	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6378	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6480	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 73 00 69 00 76 00 63 00 69 00 63 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	<SystemManufacturer>sivcic, Inc.</SystemManufacturer>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6586	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6590	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6594	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 73 00 69 00 76 00 63 00 69 00 63 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	<SystemProductName>sivcic7,1</SystemProductName>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6690	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6694	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6698	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6826	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 36 00 33 00 35 00 31 00 39 00 38 00 33 00 33 00 37 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	<OSInstallDate>1635198337</OSInstallDate>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	2	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	6916	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7018	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7022	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7026	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7100	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	</SystemInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7146	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	<SecureBootState>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7188	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	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7284	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7288	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7290	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	</SecureBootState>	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7326	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7330	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7332	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	<Integrator>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7356	4	0d 00 0a 00		success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7360	2	09 00		success or wait	6	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7364	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7608	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7612	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7614	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	</Integrator>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7640	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7644	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7646	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 33 00 2d 00 30 00 33 00 2d 00 31 00 39 00 54 00 30 00 37 00 3a 00 32 00 36 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-03-19T07:26:59Z">	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7746	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7750	2	09 00		success or wait	2	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	7754	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 38 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 00 36 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 34 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 34 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="281" PID="5764" UptimeMS="1046" TimeSinceCreationMS="1046" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8016	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8020	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8024	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8050	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	</ProcessTimelines>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8094	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	<ReportInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8132	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8136	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8140	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 66 00 32 00 35 00 64 00 35 00 33 00 61 00 2d 00 61 00 39 00 31 00 63 00 2d 00 34 00 39 00 38 00 36 00 2d 00 61 00 61 00 31 00 34 00 2d 00 66 00 30 00 61 00 32 00 36 00 65 00 39 00 61 00 31 00 61 00 33 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ff25d53a-a91c-4986-aa14-f0a26e9a1a37</Guid>	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8238	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8242	2	09 00		success or wait	2	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8246	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 33 00 2d 00 30 00 33 00 2d 00 31 00 39 00 54 00 30 00 37 00 3a 00 32 00 36 00 3a 00 35 00 39 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	<CreationTime>2023-03-19T07:26 :59Z</CreationTime>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8348	2	09 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8350	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	</ReportInformation>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8390	4	0d 00 0a 00		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA1.tmp.WERInternalMetadata.xml	8394	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	</WERReportMetadata>	success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp.xml	0	4756	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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 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 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 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	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441\Report.wer	0	2	fd fd		success or wait	1	6A5D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	157	6A5D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_ChromeFIX_errorM_b23b12b73ca7fdfaf9d7b6fd85cedf5e91158b2c_eaf10766_16b01441\Report.wer	10384	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 36 00 37 00 38 00 36 00 32 00 38 00 32 00 34 00 36 00	MetadataHash=-1678628246	success or wait	1	6A5D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	success or wait	1	6A5F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6A5F1FB2	RegCreateKeyExW
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6A5D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	ProgramId	unicode	0006f204cf76628a2937759c3b18080ecd3e00001a08	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	FileId	unicode	0000a9282e204443fed6e0be28e8e2dfe7c927706428	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	LowerCaseLongPath	unicode	c:\users\user\desktop\chromefix_errormem.exe	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	LongPathHash	unicode	chromefix_errorm|887ab9db	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	Name	unicode	chromefix_errormem.exe	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	Publisher	unicode	typists tripwire	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	Version	unicode	1.211.102.5	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	BinFileVersion	unicode	1.211.102.5	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	BinaryType	unicode	pe32_i386	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	ProductName	unicode	squirrelled cars	success or wait	1	6A5F36BF	unknown

Copyright Joe Security LLC 2023

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	ProductVersion	unicode	1.211.102.5	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	LinkDate	unicode	03/18/2023 08:03:54	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	BinProductVersion	unicode	1.211.102.5	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	Size	B	00 E0 03 00 00 00 00 00	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	Language	dword	2074	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	IsPeFile	dword	1	success or wait	1	6A5F36BF	unknown
\REGISTRY\A\{aeaca1be-77d4-13c5-86cc-78b3d48a0305}\Root\InventoryApplicationFile\chromefix_errorm|887ab9db	IsOsComponent	dword	0	success or wait	1	6A5F36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 0C 5D 08 98 02 00 00 00 08 00 00 00 0C 5D 08 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6A5F1FE8	RegSetValueExW

Disassembly

No disassembly

Copyright Joe Security LLC 2023