ID: 1459509
Sample Name: file.exe
Cookbook: default.jbs
Time: 14:39:07
Date: 19/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

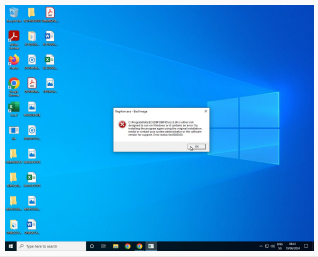
Windows Analysis Report

file.exe

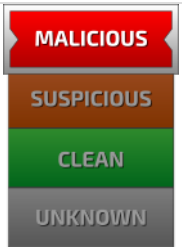
Overview

General Information

Sample name:	file.exe
Analysis ID:	1459509
MD5:	2a042e0136d2…
SHA1:	d3f5304872ff4b..
SHA256:	65746b8a8fddc..
Tags:	exe
Infos:	



Detection



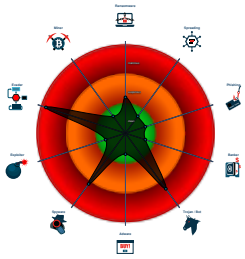
Vidar

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected Powershell download…
- Yara detected Vidar stealer
- AI detected suspicious sample
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Contains functionality to inject code…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5572 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 2A042E0136D2125E744724A757F33950)
  - RegAsm.exe (PID: 8 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
  - RegAsm.exe (PID: 2060 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
  - RegAsm.exe (PID: 3872 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" MD5: 0D5DF43AF2916F47D00C1573797C1A13)
  - WerFault.exe (PID: 6880 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5572 -s 336 MD5: C31336C1EFC2CCB44B4326EA793040F2)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	http://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Vidar


```
{
  "C2 url": [
    "https://steamcommunity.com/profiles/76561199699680841",
    "https://t.me/memve4erin"
  ],
  "Botnet": "673ad4d1558c47b58d4f59c1d86488e2"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.2942073770.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000003.00000002.2942073770.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x23208:$s1: JohnDoe • 0x23200:$s2: HAL9TH
00000000.00000002.1828525742.000000000100A000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000003.00000002.2942073770.0000000000453000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Process Memory Space: file.exe PID: 5572	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.RegAsm.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
3.2.RegAsm.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x22408:$s1: JohnDoe • 0x22400:$s2: HAL9TH
3.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
3.2.RegAsm.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x23208:$s1: JohnDoe • 0x23200:$s2: HAL9TH
0.2.file.exe.fd0000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

AI detected suspicious sample

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

Country aware sample found (crashes after keyboard check)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Yara detected Powershell download and execute

Allocates memory in foreign processes

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Searches for specific processes (likely to inject)

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Vidar stealer

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

Remote Access Functionality

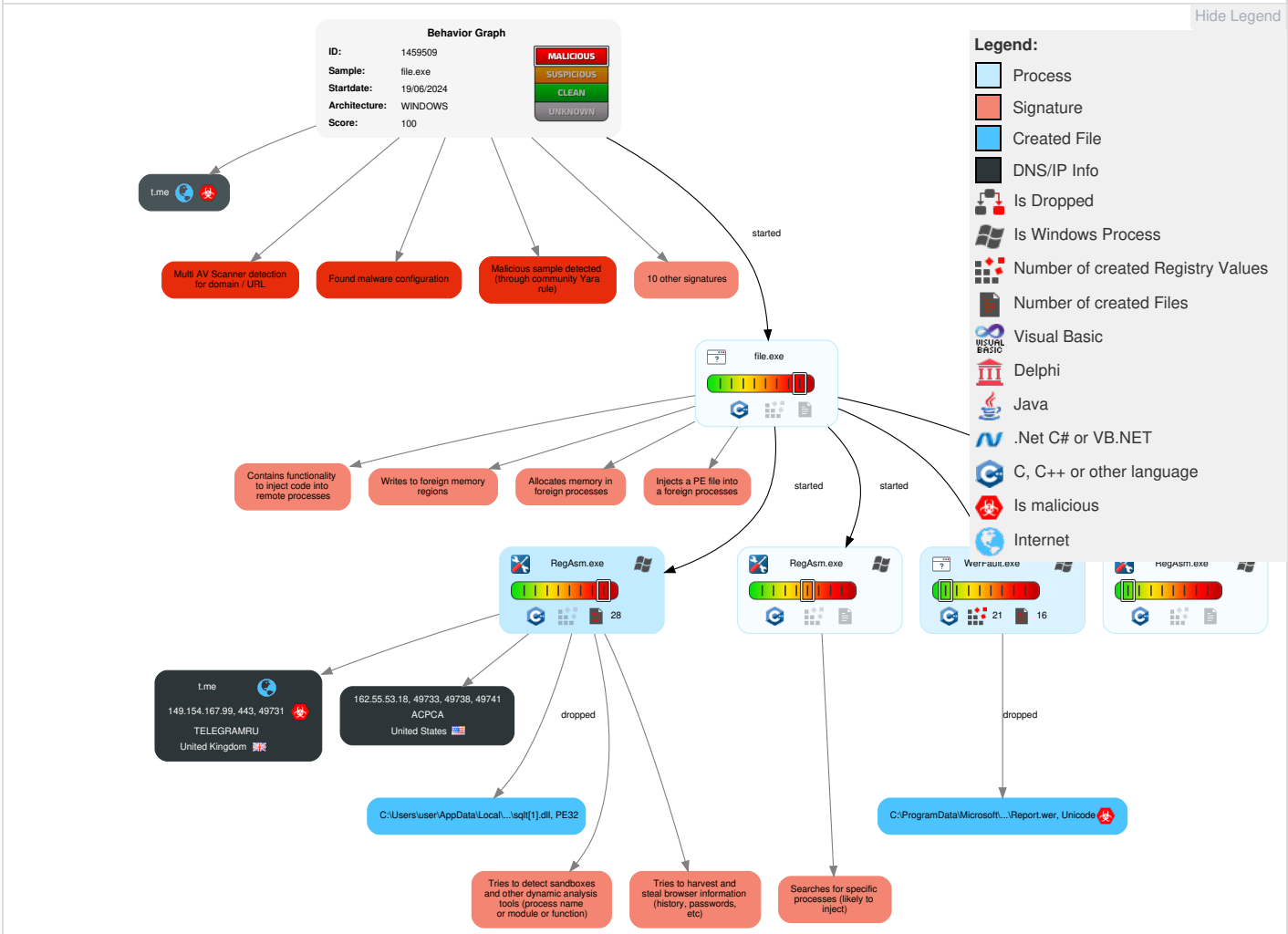
Yara detected Vidar stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Credentials	Domains	Default Accounts	1 Native API	Boot or Logon Initialization Scripts	5 1 1 Process Injection	2 Obfuscated Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	2 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Masquerading	NTDS	5 4 System Information Discovery	Distributed Component Object Model	Input Capture	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Virtualization/Sandbox Evasion	LSA Secrets	1 5 1 Security Software Discovery	SSH	Keylogging	1 3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	5 1 1 Process Injection	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	Compile After Delivery	DCSync	1 2 Process Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

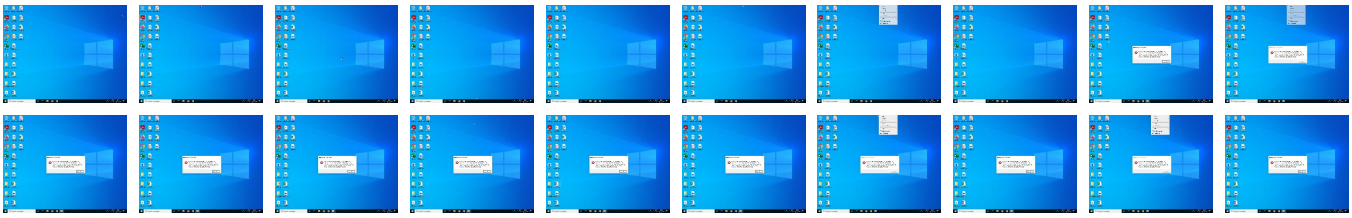
Behavior Graph



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
file.exe	38%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZVZFKMB9\sqlt[1].dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
t.me	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://upx.sf.net	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/A	100%	Avira URL Cloud	malware	
http://https://t.me/	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/softokn3.dllEdge	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000FID	0%	Avira URL Cloud	safe	
http://https://t.me/	0%	Virustotal		Browse
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/B	100%	Avira URL Cloud	malware	
http://https://t.me/memve4erin	100%	Avira URL Cloud	malware	
http://https://t.me/memve4erin	2%	Virustotal		Browse
http://https://162.55.53.18:9000/softokn3.dll10.15;	100%	Avira URL Cloud	malware	
http://https://web.telegram.org	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/B	4%	Virustotal		Browse
http://https://162.55.53.18:9000/freebl3.dllu	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/sqlt.dll	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/chrome_newtab	0%	Virustotal		Browse
http://https://web.telegram.org	0%	Virustotal		Browse
http://https://duckduckgo.com/ac/?q=	0%	Virustotal		Browse
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000646ff6le	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/46ff6le	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/msvcp140.dll	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/tm	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/sqlt.dll	16%	Virustotal		Browse
http://https://162.55.53.18:9000/softokn3.dll	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/msvcp140.dllEdge	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	0%	Avira URL Cloud	safe	
http://https://t.me/memve4erin&	0%	Avira URL Cloud	safe	
http://https://t.me/m	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/msvcp140.dll	11%	Virustotal		Browse
http://https://162.55.53.18:9000/vcruntime140.dllUser	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/p	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/MH	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/msvcp140.dllEdge	11%	Virustotal		Browse
http://https://162.55.53.18:9000/l	100%	Avira URL Cloud	malware	
http://www.sqlite.org/copyright.html.	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/freebl3.dllsposition:	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://t.me/m	0%	Virustotal		Browse
http://https://162.55.53.18:9000/l	11%	Virustotal		Browse
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/bW	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/vcruntime140.dlle	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/	100%	Avira URL Cloud	malware	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Virustotal		Browse
http://https://162.55.53.18:9000/sqlt.dllB	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000al	0%	Avira URL Cloud	safe	
http://www.sqlite.org/copyright.html.	0%	Virustotal		Browse
http://https://162.55.53.18:9000/ZG	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000tel	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/	16%	Virustotal		Browse
http://https://162.55.53.18:9000/nss3.dlloft	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000ming	0%	Avira URL Cloud	safe	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016ost.exe	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/vcruntime140.dll	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	0%	Virustotal		Browse
http://https://162.55.53.18:9000/Zm	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000nbfoldnt-Disposition:	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/$	100%	Avira URL Cloud	malware	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Virustotal		Browse
http://https://162.55.53.18:9000/freebl3.dll	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/vcruntime140.dllA	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/cG4	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/vcruntime140.dllppet	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/nss3.dllJ	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/softokn3.dll2	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:90001234567890hrome	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/nss3.dll	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/4	100%	Avira URL Cloud	malware	
http://https://162.55.53.18/	100%	Avira URL Cloud	malware	
http://https://steamcommunity.com/profiles/76561199699680841	100%	Avira URL Cloud	malware	
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	0%	Avira URL Cloud	safe	
http://https://162.55.53.18:9000/freebl3.dll~	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/mozglue.dll	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000/.53.18:9000/	100%	Avira URL Cloud	malware	
http://https://162.55.53.18:9000tacrosoft	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t.me	149.154.167.99	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://t.me/memve4erin	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
https://steamcommunity.com/profiles/76561199699680841	true	• Avira URL Cloud: malware	unknown

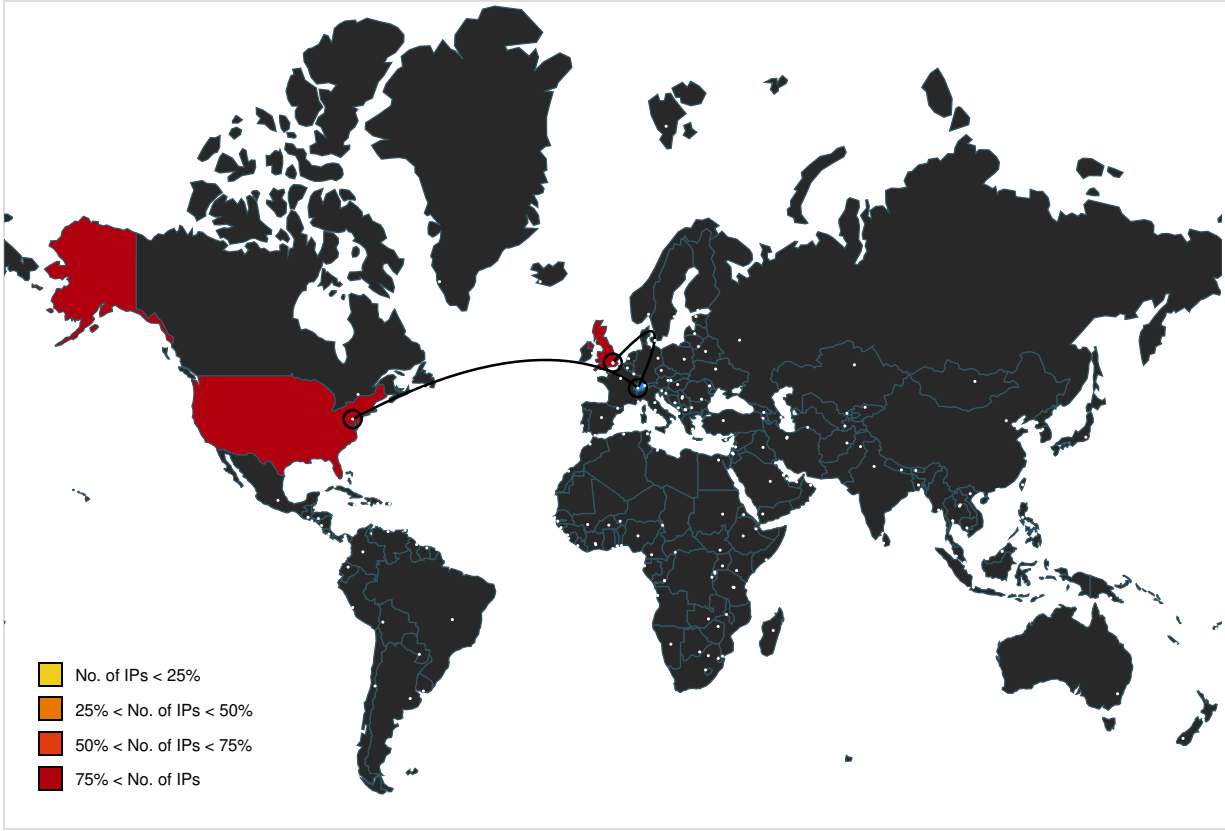
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	BAEHIE.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://t.me/	RegAsm.exe, 00000003.00000002.2942656368.0000000000F7A000.00000004.00000020.00020000.00000000.sdmp	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000FID	RegAsm.exe, 00000003.00000002.2942073770.0000000000453000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/softokn3.dllEdge	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/A	RegAsm.exe, 00000003.00000002.2942919191.00000000010BD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	BAEHIE.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/B	RegAsm.exe, 00000003.00000002.2942919191.00000000010BD000.00000004.00000020.00020000.00000000.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://web.telegram.org	RegAsm.exe, 00000003.00000002.2942073770.0000000000453000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942656368.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/softokn3.dll10.15;	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/freebl3.dllu	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/sqlt.dll	RegAsm.exe, 00000003.00000002.2942073770.0000000000491000.00000040.00000400.00020000.00000000.sdmp	false	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	BAEHIE.3.dr	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	RegAsm.exe, 00000003.00000002.2942073770.00000000004D5000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp, GDBFHD.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000646ff6le	RegAsm.exe, 00000003.00000002.2942073770.0000000000453000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.00000000004B6000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/46ff6le	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/msvcp140.dll	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/tm	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/softokn3.dll	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	RegAsm.exe, 00000003.00000002.2942073770.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/msvcp140.dllEdge	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	GDBFHD.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	BAEHIE.3.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t.me/memve4erin&	RegAsm.exe, 00000003.00000002.2942656368.0000000000FD1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/m	RegAsm.exe, 00000003.00000002.2942656368.0000000000F7A000.00000004.00000020.00020000.00000000.sdmp	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/vcruntime140.dllUser	RegAsm.exe, 00000003.00000002.2942073770.0000000000453000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/p	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/MH	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/l	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.sqlite.org/copyright.html.	RegAsm.exe, 00000003.00000002.2949605614.000000001B61D000.00000002.00001000.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2943981511.0000000015676000.00000004.00000020.00020000.00000000.sdmp, sqlt[1].dll.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/freebl3.dllsposition:	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	BAEHIE.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/bW	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/vcruntime140.dlle	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/sqlt.dllB	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000al	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.0000000000497000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/ZG	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000tel	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	BAEHIE.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://upx.sf.net	Amcache.hve.6.dr	false	• URL Reputation: safe	unknown
http://https://162.55.53.18:9000/nss3.dlloft	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	RegAsm.exe, 00000003.00000002.2942073770.00000000004D5000.00000040.00000400.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp, GDBFHD.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000ming	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016ost.exe	RegAsm.exe, 00000003.00000002.2942073770.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	BAEHIE.3.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://162.55.53.18:9000/vcruntime140.dll	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	BAEHIE.3.dr	false	• URL Reputation: safe	unknown
http://https://162.55.53.18:9000/Zm	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000nbfoldnt-Disposition:	RegAsm.exe, 00000003.00000002.2942073770.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/$	RegAsm.exe, 00000003.00000002.2942794241.0000000001009000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/vcruntime140.dllA	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/freebl3.dll	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/cG4	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/vcruntime140.dllppet	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/nss3.dllJ	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000	RegAsm.exe, 00000003.00000002.2942656368.0000000000FF2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/softokn3.dll2	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:90001234567890hrome	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/nss3.dll	RegAsm.exe, 00000003.00000002.2942919191.00000000010E2000.00000004.00000020.00020000.00000000.sdmp, RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/4	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18/	RegAsm.exe, 00000003.00000002.2942794241.0000000001009000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	GDBFHD.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://162.55.53.18:9000/freebl3.dll~	RegAsm.exe, 00000003.00000002.2942919191.00000000010CF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000/mozglue.dll	RegAsm.exe, 00000003.00000002.2942073770.000000000056E000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	BAEHIE.3.dr	false	• URL Reputation: safe	unknown
http://https://162.55.53.18:9000/.53.18:9000/	RegAsm.exe, 00000003.00000002.2942919191.00000000010BD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://162.55.53.18:9000tacrosoft	RegAsm.exe, 00000003.00000002.2942073770.00000000004D5000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.55.53.18	unknown	United States		35893	ACPCA	false
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1459509
Start date and time:	2024-06-19 14:39:07 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/15@1/2
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 98% • 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, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 95.101.54.203, 2.16.202.128, 95.101.54.194, 95.101.54.130, 2.16.202.121, 95.101.54.209, 95.101.54.144, 95.101.54.139, 95.101.54.202, 20.42.73.29
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, login.live.com, slscr.update.microsoft.com, ctldl.windowsupdate.com.delivery.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, a767.dspw65.akamai.net, wu-b-net.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, download.windowsupdate.com.edgesuite.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:40:07	API Interceptor	1x Sleep call for process: RegAsm.exe modified
08:40:13	API Interceptor	1x Sleep call for process: WerFault.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\ECGDBFCBKFID\AEBGHD

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7YItnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26

SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903
SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621(3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\ProgramData\ECGDBFCBKFID\BAEHIE

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3 EB
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\ProgramData\ECGDBFCBKFID\CBKFBA

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88 F7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j..... ....

C:\ProgramData\ECGDBFCBKFID\DBGHJE

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE

SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F798 38
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\ECGDBFCBKFID\DGHIDH

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	modified
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4..... ....

C:\ProgramData\ECGDBFCBKFID\GDBFHD

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\ProgramData\ECGDBFCBKFID\KKEHDB

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de\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):	0.7085213233949067
Encrypted:	false
SSDEEP:	192:M7JhBl4vVPl+0p4iZI3jXqzuiFuZ24lO8TVB:y3oVNlp4iKj6zuiFuY4lO8X
MD5:	A33DBE13115559E3B20FE7A91AB745E5
SHA1:	E3561DBB2B9DC413FD262CE495EAFD8FCB066606
SHA-256:	58CF440D304337042E25AEEA912BDBB986A90BDD6EBB9DE27F4C1DE487EF7B36
SHA-512:	3431CCD9A3347E16458FE3333F769664662C800D9E090BEA3278A11CC8DA4D3D2618E2BF9A56E5935FDA4CAA39513E814485593092598592EDDF4A664D7FBAA
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.6.3.2.7.4.3.9.9.4.8.9.4.1.3.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.6.3.2.7.4.3.9.9.7.8.6.2.7.2.3.....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.=.2.d.8.c.e.c.7.4.-.3.5.4.d.-.4.6.0.a.-.9.5.a.d.-.b.f.7.8.8.4.e.f.0.9.d.e.....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.=.8.9.3.2.b.9.b.c.-.a.5.b.1.-.4.9.4.e.-.9.2.8.5.-.6.f.5.2.2.8.a.3.d.a.f.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.c.4.-.0.0.0.1.-.0.0.1.4.-.e.c.7.2.-.d.1.c.b.4.5.c.2.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.e.4.9.2.d.7.6.8.e.7.9.7.3.1.6.2.4.b.c.d.f.2.e.7.6.1.5.f.9.1.8.0.0.0.0.f.f.f.f.!.0.0.0.0.d.3.f.5.3.0.4.8.7.2.f.f.4.b.7.9.5.c.d.e.4.8.9.1.4.f.a.4.d.8.1.7.6.8.a.b.b.a.5.d.!.f.i.l.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.4././.0.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 19 12:39:59 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	43270
Entropy (8bit):	1.8018423576157767
Encrypted:	false
SSDEEP:	192:KDVZHTdMLtO/n4s+kTyBTq7vnl1s/hbM9RcMJP:IVB5M8wtkEOznI1ehbM1
MD5:	AD261D87896F54820D9B230CEDCFA287
SHA1:	77F3D1A51A187415703A74B03C22FF9918E07679
SHA-256:	B9336CF50D5C97087EBBE3D7574DDF397BE47A2E3B1BD53374B8B942765BBAC8
SHA-512:	9EAFE33D3AA361BEEBF554323CE25FBE6DC6C1BC763B88C3771333D7C58DB356F3DEFA6A1DC29BB06BAC505FC18017DA2AAB9DC5306AF5C08F00FB001770 8F1
Malicious:	false
Preview:	MDMP..a..... .....rf.....0.....$...Z!.....T.....8.....T.....eJ.....GenuineI ntel.....T.....rf.....0.....,...E.a.s.t.e.r.n. .S.t.a.n.d.a.r.d. .T.i.m.e.....E.a.s.t.e.r.n. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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):	8326
Entropy (8bit):	3.695451458569435
Encrypted:	false
SSDEEP:	192:R6l7wVeJnCJ6O76Y9eSU9ngmfBOJJQpr189bVHHsfrHHm:R6lXJk6q6YkSU9ngmf0JJXVHMfTG
MD5:	A73CA148A343A6488103EB6DA5B0B24F
SHA1:	F5BF5D4ABC240C01AF4E83FF7C9C7018C321824B
SHA-256:	808EE5142C537E69CA2B0DF54D1252ADC7903D629BCF5702827C0BA617FE97AB
SHA-512:	147F8D4901E3958A52C597FD383AB3BFBE4078865FA5A42931F19456C9D4CBFF5FAD8BAF9E9CC242D057BFE3542FE900172D29F636C3345C021577AA517D592
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.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.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.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.>.2.0.5.7.<./.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.>.5.5.7.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD52.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4605
Entropy (8bit):	4.481762253623764
Encrypted:	false
SSDEEP:	48:cvIwWl8zs2Jg77aI9HhzSWpW8VYsYm8M4JTgFQV+q8wgnzgSO2d:uIjfMI7Lf7VAJZVOn/O2d
MD5:	B9D33F03AC07847C1A74E1816C865F0C
SHA1:	17AAEB63BE85042614E78C8E8221D711BFA65CB7
SHA-256:	29098E1774F6903A1DBBB85B669E95764F9493D95F097CAE0019768A69B0E879
SHA-512:	2A68292407E459486F88E982F7CA65ABFBA0AFAC5FB61C07E826BCC0C1C6F2F82D645C484C48DEC1DAAA521103D3F9F9CE5053BDC26C4A7AA1A89FFFB5329BF0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <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="374622" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 71954 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	71954
Entropy (8bit):	**7.996617769952133**
Encrypted:	**true**
SSDEEP:	1536:gc257bHnClJ3v5mnAQEBP+bfnW8Ctl8G1G4eu76NWDdB34w18R5cBWcJAm68+Q:gp2ld5jPqW8LgeulxB3fgcEfDQ
MD5:	49AEBF8CBD62D92AC215B2923FB1B9F5
SHA1:	1723BE06719828DDA65AD804298D0431F6AFF976
SHA-256:	B33EFCB95235B98B48508E019AFA4B7655E80CF071DEFABD8B2123FC8B29307F
SHA-512:	BF86116B015FB56709516D686E168E7C9C68365136231CC51D0B6542AE95323A71D2C7ACEC84AAD7DCECC2E410843F6D82A0A6D51B9ACFC721A9C84FDD8775B
Malicious:	false
Preview:	MSCF.....,.....I.....XaK .authroot.stl.[.i..6..CK..<Tk.....4.cl!Kg..E..*Y.f_..".$mR"$.J.E.KB."..rKv.."{.g....3.W.....c..9.s...=....y6#..x.....D.....\(.#.s.!.A.....cd.c.....+^.ov...n.....3BL..0.....BPUR&.X..02.q...R...J.....w.....b.vy>....-.&..(..oe.."."...J9...0U.6J..|U..S.....M.F8g...=.....p.....I.?3.J.x.G.Ep..$g..tj.....)v]9(:.)W.8.Op.1Q..:.nPd.....7.7..M].V F..g.....12..!7(...B.....h.RZ.....I.<.....6..Z^.`p?... .p.Gp.#.'.X.....|!.8.....".m.49r?.I...g...8.v.....a``.g.R4.i...J8q....NFW,E.6Y....!.o5%.Y.....R..<..S9....r....WO...(.....F..Q=*....-..7d..O(....-..+k.....K.....{Q....Z..j._.E...QZ.~.\.^.....N.9.k..O.}dD.b1r...[}/....T..E..G..c.|.c.&>?..^t. ..;..X.d.E.0G....[Q.*,*.....#.Dp..L.o|#syc.J.....}G-.ou6.=52..XWi=...m.....^u.....c..fc?&pR7S5....I...j.G.....j.j..Tc.El.....B.pQ.,Bp....j...9g.. >..s..m#.Nb.o_u.M.V.....\#...v..Mo\sF..s....Y...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1356875516282012
Encrypted:	false
SSDEEP:	6:kKogna9UswDLL+N+SkQlPlEGYRMY9z+4KlDA3RUebT3:l1DnLNkPlE99SNxAhUe/3
MD5:	643A04DE806F367F95FA2C2372EAFDCE
SHA1:	690912B614D8E6C79F4788579A7F7416B33ADC70
SHA-256:	51837F0C94CE19779EFD1BDC1E37E46F06002A3D7AB02248C8FED4970831E2D5
SHA-512:	75E0579CD381174B4F406F10AE5233186608B13CA54AB860732485169DFEB78061D047DDB575C4F3A20D816BD7B5F22803A948380C1F8D2D69E8E3ABD09710B4
Malicious:	false
Preview:	p..... .....m}.E...(..... .....G..@.....&.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".a.7.2.8.2.e.b.4.0.b.1.d.a.1.::.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZVZFKMB9\sqlt[1].dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353

Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E57032 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.Z.Y.Z.Y.Z.Y...Z.n.Y...\..Y...]...Y...X.Y.Y.Z.X..Y.O.\.E.Y. O.].U.Y.O.Z.L.Y.l3].[.Y.l3Y.[.Y.l3..[.Y.l3[.[.Y.RichZ.Y.....PE..L...i.`e.....!...%.. .....{D..... .....%.....@.....#..6....$.(.....$..... .....$.....`.#.8.....x.#.@.....$.....text...G. ....`.rdata..."..... ..$... .....@..@.data...4|... $..b....#.....@....idata.... ....$.....^$.....@..@.00cfg.....$.....p$.....@..@.rsrc.....$.....r$.....@..@.reloc..5.....$.....$.....@..B.....

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):	1835008
Entropy (8bit):	4.465312700633052
Encrypted:	false
SSDEEP:	6144:/IXfpi67eLPU9skLmb0b4+WSPKaJG8nAgejZMMhA2gX4WABl0uNPdwBCswSbS:wXD94+WlLZMM6YFH1+S
MD5:	6D91DFAE854B49B66485D228E7E0BF0C
SHA1:	5662AFA897D945CD7F006DA86596DE6A8D3EBD95
SHA-256:	EDD8F426181C009364A73CF0F2BE9CA205BD9002CD4927F5BA159B503BA71523
SHA-512:	CAC1142CE303A9B7AE3404F49E9A5FB2B14CDAC761EB805D5FC2C3EB2C7BF37F0197CA1F3CD6AA2B80987D9FB3F70A7F2E702A1C4E7C27E15D50AAFAEBF0 2CDB
Malicious:	false
Preview:	regf6...6....\.Z..... .....\.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....c...b...#.....c...b...#.....c...b...#.....rmtm.O#.E..... ....5..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.474701129164594
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:	file.exe
File size:	455'680 bytes
MD5:	2a042e0136d2125e744724a757f33950
SHA1:	d3f5304872ff4b795cde48914fa4d81768abba5d
SHA256:	65746b8a8fddc5dfb1602a3a5605cd039476bab5e66076bc729b987793986e0e
SHA512:	428e5cd961441fbfe4851dcef4431cad371673813028a631c5ca6cb7bda6d74d4f63b2d45689cd8d6c8cb6fc92dd1eb09bf4e307a93df1c9600c235951a4f1e8
SSDEEP:	6144:rAyIw/Vb6XOM8xYKn+TKRQGXHqF74UyM1nblXV8a0+lESfFa0l06qiXyf9RIR3pf:rAyI6b6XOMCT+B4Uyn6ESVlvqiKI5f
TLSH:	4DA4E01074828072D5A61A3306B4DBB95A7EB9344B618ECFA3D54F7EDF302C197325AB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....bC..1C..1C..1...0R..1...0...1...0U..1.Y.0Q..1.Y.0V..1...0J..1C..1...1.Y.0...1.Z.0B..1.Z.0B..1.Z.0B..1RichC..1.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General	
Entrypoint:	0x40c1c7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6672C39D [Wed Jun 19 11:40:13 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	4d71c6568cd912923f8bc2058a57f65f

Entrypoint Preview
Instruction
call 00007F702141E599h
jmp 00007F702141DC4Fh
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007F702141DDEBh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007F702141DDDCh
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007F702141DDDEh
add edx, 28h
cmp edx, esi
jne 00007F702141DDBCh
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007F702141DDCBh
push esi
call 00007F702141E89Fh
test eax, eax
je 00007F702141DDF2h
mov eax, dword ptr fs:[00000018h]
mov esi, 0046F3D4h

Instruction
mov edx, dword ptr [eax+04h]
jmp 00007F702141DDD6h
cmp edx, eax
je 00007F702141DDE2h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007F702141DDC2h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007F702141DDD9h
mov byte ptr [0046F3D8h], 00000001h
call 00007F702141E095h
call 00007F7021420EE2h
test al, al
jne 00007F702141DDD6h
xor al, al
pop ebp
ret
call 00007F702142E4A7h
test al, al
jne 00007F702141DDDCh
push 00000000h
call 00007F7021420EE9h
pop ecx
jmp 00007F702141DDBBh
mov al, 01h
pop ebp
ret
push ebp
mov ebp, esp
cmp byte ptr [0046F3D9h], 00000000h
je 00007F702141DDD6h
mov al, 01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x38dc0	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x38e0c	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x71000	0x206c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x36cd8	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x36c18	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2e000	0x160	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2c360	0x2c400	48ebe9f7db94e39cc36c31d49f896c3c	False	0.5570930437853108	data	6.657127142960566	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2e000	0xb5fc	0xb600	0cf0f9b30a372925a0871d8a6edaf1b5	False	0.42301253434065933	data	5.04202350165611	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3a000	0x35fe8	0x34e00	4fc4cf94d711a2509e54fb9c025c868e	False	0.9842780363475178	data	7.983738010153567	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bSs	0x70000	0x4ac	0x600	f929bf25d4c42bd01cdad568b5fe4d8a	False	0.4791666666666667	data	5.111291762588542	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x71000	0x206c	0x2200	3e1192bfa628a7fe9ce4ea609327c4e6	False	0.7296645220588235	data	6.424471018903299	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

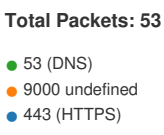
DLL	Import
GDI32.dll	SetPixel
USER32.dll	GetDC, DestroyWindow, ReleaseDC
ADVAPI32.dll	GetNumberOfEventLogRecords, DeleteAce
KERNEL32.dll	WriteConsoleW, GetProcessHeap, CreateFileW, HeapSize, CloseHandle, WaitForSingleObject, CreateThread, VirtualAlloc, GetConsoleWindow, GetCurrentThreadId, WideCharToMultiByte, MultiByteToWideChar, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, QueryPerformanceCounter, EncodePointer, DecodePointer, LCMapStringEx, GetSystemTimeAsFileTime, GetModuleHandleW, GetProcAddress, GetCPInfo, IsProcessorFeaturePresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, GetCurrentProcessId, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, SetStdHandle, RaiseException, RtlUnwind, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetModuleHandleExW, GetStdHandle, WriteFile, GetModuleFileNameW, ExitProcess, HeapAlloc, HeapFree, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetFileType, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEndOfFile

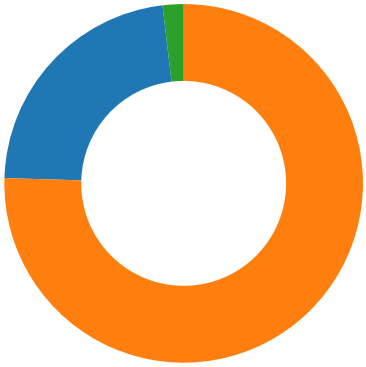
Exports

Name	Ordinal	Address
AsuxuiHAuiiua	1	0x409310

Network Behavior

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 19, 2024 14:39:59.852648020 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:39:59.852751017 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:39:59.852835894 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:39:59.887254000 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:39:59.887291908 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.527199030 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.527314901 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.591753006 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.591808081 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.592763901 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.592848063 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.594978094 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.636522055 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.779308081 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.779371977 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.779407978 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.779475927 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.779525042 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.779550076 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.779562950 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.779639959 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.781646013 CEST	49731	443	192.168.2.4	149.154.167.99
Jun 19, 2024 14:40:00.781682014 CEST	443	49731	149.154.167.99	192.168.2.4
Jun 19, 2024 14:40:00.787695885 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:00.792666912 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:00.792748928 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:00.793065071 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:00.797921896 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:01.438410044 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:01.438441992 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:01.438474894 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:01.438524961 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:02.400815964 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:02.405736923 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:02.592015982 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:02.592123032 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:02.592550993 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:02.597348928 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:03.043494940 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:03.043572903 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:03.047522068 CEST	49738	9000	192.168.2.4	162.55.53.18

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 19, 2024 14:40:03.052671909 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:03.052781105 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:03.053028107 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:03.058120012 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:03.684803963 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:03.684912920 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:03.692576885 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:03.697453022 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:03.731571913 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:03.738267899 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.312442064 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.312650919 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.313782930 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.314119101 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.319207907 CEST	9000	49733	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.319266081 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.319297075 CEST	49733	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.319340944 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.319617987 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.325268030 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.976289988 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.976355076 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.976794958 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.978588104 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:04.981465101 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:04.983596087 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:05.671540976 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:05.671556950 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:05.671566010 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:05.671673059 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:05.673285007 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:05.673738003 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:05.680844069 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:05.680927992 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:05.681200027 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:05.681315899 CEST	9000	49738	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:05.681360960 CEST	49738	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:05.685951948 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.321352959 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.321444035 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.321836948 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.326610088 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.347815990 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.352690935 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.949598074 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.949621916 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.949632883 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.949640989 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.949646950 CEST	9000	49742	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.949807882 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.949807882 CEST	49742	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.951541901 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.952148914 CEST	49744	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.956809998 CEST	9000	49741	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.956892014 CEST	49741	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.958511114 CEST	9000	49744	162.55.53.18	192.168.2.4
Jun 19, 2024 14:40:06.958599091 CEST	49744	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.958859921 CEST	49744	9000	192.168.2.4	162.55.53.18
Jun 19, 2024 14:40:06.963690996 CEST	9000	49744	162.55.53.18	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 19, 2024 14:39:59.810946941 CEST	50394	53	192.168.2.4	1.1.1.1
Jun 19, 2024 14:39:59.820652962 CEST	53	50394	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 19, 2024 14:39:59.810946941 CEST	192.168.2.4	1.1.1.1	0x5593	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false

DNS Answers

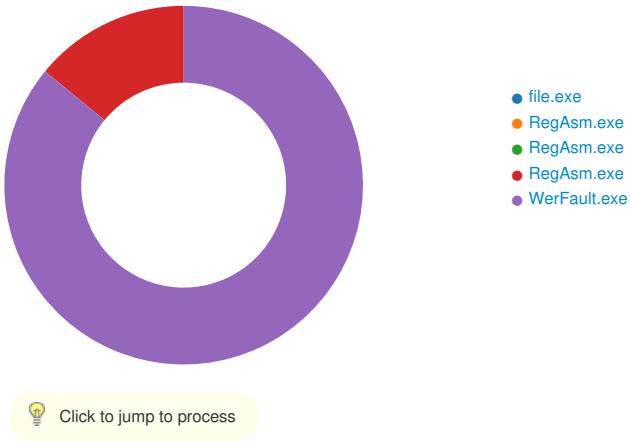
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 19, 2024 14:39:59.820652962 CEST	1.1.1.1	192.168.2.4	0x5593	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- t.me

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **5572**, Parent PID: **2580**

General

Target ID:	0
Start time:	08:39:58
Start date:	19/06/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"

Imagebase:	0xfd0000
File size:	455'680 bytes
MD5 hash:	2A042E0136D2125E744724A757F33950
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.1828525742.000000000100A000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

Analysis Process: RegAsm.exe PID: **8**, Parent PID: **5572**

General	
Target ID:	1
Start time:	08:39:59
Start date:	19/06/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Imagebase:	0x3a0000
File size:	65'440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: RegAsm.exe PID: **2060**, Parent PID: **5572**

General	
Target ID:	2
Start time:	08:39:59
Start date:	19/06/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Imagebase:	0x330000
File size:	65'440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: RegAsm.exe PID: **3872**, Parent PID: **5572**

General	
Target ID:	3
Start time:	08:39:59
Start date:	19/06/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"

Imagebase:	0x7f0000
File size:	65'440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000002.2942073770.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation, Description: Detects executables containing potential Windows Defender anti-emulation checks, Source: 00000003.00000002.2942073770.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000002.2942073770.0000000000453000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	417E5E	CreateDirectoryA
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	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
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	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
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	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
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	405034	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405034	HttpSendRequestA
C:\ProgramData\ECGDBFCBKFID\AEBGHD	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4073EE	CopyFileA
C:\ProgramData\ECGDBFCBKFID\GDBFHD	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40DD1A	CopyFileA
C:\ProgramData\ECGDBFCBKFID\CBKFBA	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40CEBF	CopyFileA
C:\ProgramData\ECGDBFCBKFID\BAEHIE	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40DA81	CopyFileA
C:\ProgramData\ECGDBFCBKFID\DBGHJE	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40DD1A	CopyFileA
C:\ProgramData\ECGDBFCBKFID\KKEHDB	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40CEBF	CopyFileA
C:\ProgramData\ECGDBFCBKFID\DGHIDH	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40DA81	CopyFileA
C:\ProgramData\ECGDBFCBKFID\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGDBFCBKFID\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGDBFCBKFID\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGDBFCBKFID\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA
C:\ProgramData\ECGDBFCBKFID\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	404E83	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID\AEBGHD	success or wait	1	407905	DeleteFileA
C:\ProgramData\ECGDBFCBKFID\GDBFHD	success or wait	1	40DE10	DeleteFileA
C:\ProgramData\ECGDBFCBKFID\CBKFBA	success or wait	1	40D15D	DeleteFileA
C:\ProgramData\ECGDBFCBKFID\BAEHIE	success or wait	1	40DC01	DeleteFileA
C:\ProgramData\ECGDBFCBKFID\DBGHJE	success or wait	1	40DE10	DeleteFileA
C:\ProgramData\ECGDBFCBKFID\KKEHDB	success or wait	1	40D15D	DeleteFileA
C:\ProgramData\ECGDBFCBKFID\DGHIDH	success or wait	1	40DC01	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ZVZFKMB9\sqlt[1].dll	0	1024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1e fd 37 fd 5a fd 59 fd 5a fd 59 fd 5a fd 59 fd 11 fd 5a fd 6e fd 59 fd 11 fd 5c fd f3 59 fd 11 fd 5d fd 7f fd 59 fd 11 fd 58 fd 59 fd 59 fd 5a fd 58 fd 33 59 fd 4f fd 5c fd 45 fd 59 fd 4f fd 5d fd 55 fd 59 fd 4f fd 5a fd 4c fd 59 fd 6c 33 5d fd 5b fd 59 fd 6c 33 59 fd 5b fd 59 fd 6c 33 fd fd 5b fd 59 fd 6c 33 5b fd 5b fd 59 fd 52 69 63 68 5a fd 59 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7ZYZYZYZnY\Y] Y XYYZXYO\EYO]UYOZLY l3][Yl3Y[Yl3[Yl3[[YRichZY	success or wait	2296	40433D	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID\AEBGHD	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 0b 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	4073EE	CopyFileA
C:\ProgramData\ECGDBFCBKFID\GDBFHD	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	40DD1A	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID\CBKFBA	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	40CEBF	CopyFileA
C:\ProgramData\ECGDBFCBKFID\BAEHIE	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	40DA81	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID\DBGHJE	0	126976	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 02 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 0f fd 00 00 00 00 1c 0f 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40DD1A	CopyFileA
C:\ProgramData\ECGDBFCBKFID\KKEHDB	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	40CEBF	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ECGDBFCBKFID\DGHIDH	0	114688	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 05 07 fd 00 00 00 00 34 07 fd 07 fd 07 fd 07 fd 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 8$.O}4	success or wait	1	40DA81	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	66646	success or wait	1	406D43	ReadFile
C:\ProgramData\ECGDBFCBKFID\AEBGHD	0	100	success or wait	6	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\GDBFHD	0	100	success or wait	6	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\GDBFHD	0	100	success or wait	6	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\CBKFBA	0	100	success or wait	6	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\BAEHIE	0	100	success or wait	18	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\BAEHIE	0	100	success or wait	9	1B3DFE09	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	0	6648	success or wait	1	406D43	ReadFile
C:\ProgramData\ECGDBFCBKFID\DBGHJE	0	100	success or wait	6	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\DBGHJE	0	100	success or wait	12	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\DGHIDH	0	100	success or wait	10	1B3DFE09	ReadFile
C:\ProgramData\ECGDBFCBKFID\DGHIDH	0	100	success or wait	10	1B3DFE09	ReadFile

Analysis Process: WerFault.exe PID: **6880**, Parent PID: **5572**

General

Target ID:	6
Start time:	08:39:59
Start date:	19/06/2024
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5572 -s 336
Imagebase:	0xf50000
File size:	483'680 bytes
MD5 hash:	C31336C1EFC2CCB44B4326EA793040F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\b90a61cb-8325-4c79-b3a3-5a2408c6930a	delete | generic read | generic write	device	delete on close	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\022ce632-f567-4cc5-94a6-d8323247e8bb	delete | generic read | generic write	device	delete on close	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\c7674a23-1a21-4dc3-b2a7-b5cff4bc4c64	delete | generic read | generic write	device	delete on close	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\5cbda08a-c1b9-4a76-90d8-a703164fb83a	delete | generic read | generic write	device	delete on close	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD52.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\5e11e450-056e-4082-b760-44072b67ab26	delete | generic read | generic write	device	delete on close	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de\9b0d80ed-f725-4c14-b95a-1ebfe640ebfc	delete | generic read | generic write	device	delete on close	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C696C4D	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 72 66 fd 05 12 00 00 00 00 00	MDMPa rf	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	4480	6	00 00 00 00 00 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	200	1420	00 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 fd 11 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c fd 06 08 00 fd fd fd 0f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 15 00 00 fd fd 72 66 00 00 00 00 00 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 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 2c 01 00 00 45 00 61 00 73 00 74 00 65 00 72 00 6e 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 45 00 61 00 73 00 74 00 65 00 72 00 6e 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00	eJGenuineIntelTrf0,Eastern Standard TimeEastern Summer Time	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	4958	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 60 39 fd 76 28 fd 1b 03 fd fd 1b 03 08 fd 1b 03 fd 70 fd 76 23 00 00 00 46 02 00 00 fd fd 1b 03 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	+S++`9v(pv#F+	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 74 03 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd 70 fd 76 00 00 00 00 01 00 00 00 00 00 00 00 60 39 fd 76 00 00 00 00 fd 3c fd 76 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 74 fd 1b 03 00 00 00 00 00 00 1c 03 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 30 fd 1b 03 00 00 00 00 fd fd fd 76 00 00 00 00 fd fd 1b 03 00 00 00 00 00 fd fd 76 00 00 00 00 fd 01 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1b 03 00 00 00 00 fd 02 00 00 5e 13 00 00	tpv`9v<vt0vv^	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	8538	20	12 00 00 00 3c 2a fd 76 00 00 00 00 00 01 00 00 7e 22 00 00	<*v~"	success or wait	18	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	8830	256	fd fd fd fd 55 fd fd 56 57 53 fd fd 33 fd fd 75 14 fd 75 10 fd 75 0c fd 55 08 fd fd 5b 5f 5e 5d fd 10 00 fd fd 09 00 fd fd fd fd fd fd fd fd fd fd fd 38 00 00 00 00 fd fd fd fd 76 fd fd fd 20 00 fd fd 01 00 03 00 fd fd fd fd 76 fd fd fd 04 00 fd fd 02 00 00 00 fd fd fd fd 76 fd fd fd 18 00 fd fd 03 00 0a 00 fd fd fd fd 76 fd fd fd 0c 00 fd fd 04 00 0d 00 fd fd fd fd 76 fd fd fd 0c 00 fd fd 05 00 00 00 fd fd fd fd 76 fd fd fd 0c 00 fd fd 06 00 1a 00 fd fd fd fd 76 fd fd fd 24 00 fd fd 07 00 1b 00 fd fd fd fd 76 fd fd fd 28 00 fd fd 08 00 1a 00 fd fd fd fd 76 fd fd fd 24 00 fd fd 09 00 1c 00 fd fd fd fd 76 fd fd fd 14 00 fd fd 0a 00 0c 00 fd fd fd fd 76 fd fd fd 0c 00 fd fd 0b 00 00 00 fd fd fd fd 76 fd fd fd 10 00 fd fd 0c 00 00 00 fd fd fd fd 76 fd	UVWS3uuuU[_^]v vvvvvv$v(v$vvvv	success or wait	17	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	36570	1292	fd 47 fd 76 60 5c fd 76 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd fd 01 58 fd fd 01 fd fd fd fd fd 59 fd 76 fd 59 fd 76 fd fd fd fd 00 50 2e 01 00 50 2e 01 fd fd fd fd fd 00 00 00 fd fd fd fd fd 00 00 00 00 00 00 00 00 50 2e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 62 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 0e 63 01 00 00 00 00 00 00 00 00 00 fd 2d 01 fd fd fd fd 00 00 00 00 10 00 00 00 00 00 00 00 00 fd 62 01 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 2d 01 64 fd fd 01 fd fd 62 01 6c fd fd 01 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	Gv`\vXYvYvP.P.P.b c-bT-dbl	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	5674	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 18 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 14 01 fd 2a fd 76 23 00 00 00 06 02 00 00 5c fd 14 01 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++*v#\+	success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	1936	48	fd 16 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2e 01 00 00 00 00 74 fd 1b 03 00 00 00 00 fd 13 00 00 4a 7b 00 00 fd 02 00 00 fd 1e 00 00	.tJ{	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	1996	4	11 00 00 00		success or wait	17	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	4486	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	17	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	3728	752	00 00 fd 76 00 00 00 00 00 fd 00 00 fd fd 00 00 fd cb 37 40 13 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 02 61 4a 00 00 0a 00 fd 02 61 4a 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 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 00 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 5d 10 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 77 05 00 00 00 00 00 2f 75 06 00 00 00 00 00 00 00 00 00 00 00 00 00 3d 15 1a 00 00 00 00 00 03 fd 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 6d fd 05 00 00 00 00	v7@aJaJ?Zb]w/u=@m	success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	37862	5408	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 00 00 00 00 01 00 00 00 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	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCA4.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 30 07 00 00 fd 07 00 00 05 00 00 00 24 01 00 00 5a 21 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 08 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 0e 00 00 16 00 00 00 fd 00 00 00 fd 10 00 00	0$Z!T8T	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	478	138	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 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 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>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	682	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	762	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	874	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	926	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5572</Pid>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1012	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>file.exe</ImageName>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1180	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>757</Uptime>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1228	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1318	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	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1378	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1432	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 35 00 33 00 30 00 37 00 31 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>53071872</PeakVirtualSize>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1528	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 34 00 38 00 39 00 34 00 37 00 32 00 30 00 30 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>48947200</VirtualSize>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1598	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1602	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1608	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 36 00 37 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1674</PageFaultCount>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1692	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 32 00 33 00 34 00 31 00 31 00 32 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>6234112</PeakWorkingSetSize>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1798	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 32 00 33 00 30 00 30 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6230016</WorkingSetSize>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	1888	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 39 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>99104</QuotaPeakPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2000	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2004	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2010	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 30 00 32 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>91024</QuotaPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2106	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2110	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2116	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 31 00 38 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>18184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2240	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2244	2	09 00		success or wait	3	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2250	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 31 00 37 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>17912</QuotaNonPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2358	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2362	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2368	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 34 00 33 00 37 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>1437696</PagefileUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2454	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 34 00 34 00 35 00 38 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1445888</PeakPagefileUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2556	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 34 00 33 00 37 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>1437696</PrivateUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2636	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2682	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2686	2	09 00		success or wait	2	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2690	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2720	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2724	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2730	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2770	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2774	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2782	30	3c 00 50 00 69 00 64 00 3e 00 32 00 35 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2580</Pid>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2824	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2894	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2898	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2906	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	2996	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3000	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3008	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 37 00 33 00 39 00 35 00 34 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6739547</Uptime>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3056	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3060	2	09 00		success or wait	4	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3068	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3146	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3150	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3158	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3210	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3214	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3222	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3266	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3270	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3280	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3370	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3374	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3384	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3472	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 30 00 35 00 35 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>105548</PageFaultCount>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3550	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3554	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3564	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 39 00 39 00 34 00 35 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>129945600</PeakWorkingSetSize>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3678	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 39 00 35 00 32 00 37 00 38 00 30 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>129527808</WorkingSetSize>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3776	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 35 00 32 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>1152200</QuotaPeakPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	3906	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 39 00 39 00 37 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>999760</QuotaPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4018	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 38 00 36 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>86064</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4156	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 32 00 39 00 39 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>82992</QuotaNonPagedPoolUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4278	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 35 00 31 00 31 00 37 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45117440</PagefileUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4370	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 36 00 34 00 34 00 38 00 36 00 34 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>46448640</PeakPagefileUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4478	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 35 00 31 00 31 00 37 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45117440</PrivateUsage>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4564	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4620	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4670	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4708	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4756	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4802	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	4872	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>file.exe</Parameter0>	success or wait	8	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5520	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5524	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5526	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5566	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5570	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5572	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	6	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	12	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	5618	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 39 00 30 00 34 00 35 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>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6172	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6176	2	09 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6178	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6218	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6222	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6224	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6270	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 32 00 43 00 38 00 36 00 46 00 37 00 43 00 2d 00 44 00 42 00 32 00 42 00 2d 00 34 00 46 00 36 00 41 00 2d 00 39 00 35 00 41 00 44 00 2d 00 39 00 38 00 42 00 34 00 41 00 32 00 41 00 45 00 30 00 30 00 38 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>92C86F7C-DB2B-4F6A-95AD-98B4A2AE008A</MID>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6364	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6368	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6372	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 66 00 61 00 6c 00 6f 00 65 00 6f 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>faloeo, Inc.</SystemManufacturer>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6478	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6482	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6486	98	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 66 00 61 00 6c 00 6f 00 65 00 6f 00 32 00 30 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>faloeo20,1</SystemProductName>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6584	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6588	2	09 00		success or wait	2	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6592	122	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 32 00 30 00 31 00 2e 00 30 00 30 00 56 00 2e 00 32 00 30 00 38 00 32 00 39 00 32 00 32 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 32 00 31 00 31 00 32 00 31 00 31 00 38 00 34 00 32 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>VMW201.00V.20829224.B64.2211211842</BIOSVersion>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6722	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 37 00 33 00 33 00 30 00 34 00 33 00 34 00 35 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>1673304345</OSInstallDate>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6804	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6808	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6812	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 32 00 33 00 2d 00 31 00 30 00 2d 00 30 00 33 00 54 00 30 00 38 00 3a 00 35 00 37 00 3a 00 31 00 38 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>2023-10-03T08:57:18Z</OSInstallTime>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6914	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6918	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6922	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 35 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>05:00</TimeZoneBias>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	6996	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7042	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7084	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7186	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7222	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7226	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7228	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	3	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	6	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7260	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7504	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7508	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7510	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7536	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7540	2	09 00		success or wait	1	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7542	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 34 00 2d 00 30 00 36 00 2d 00 31 00 39 00 54 00 31 00 32 00 3a 00 33 00 39 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2024-06-19T12:39:59Z">	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7642	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7646	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7650	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 35 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="406" PID="5572" UptimeMS="171" TimeSinceCreationMS="171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7916	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7936	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7940	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7942	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7980	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7984	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	7986	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	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8024	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8028	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8032	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 64 00 38 00 63 00 65 00 63 00 37 00 34 00 2d 00 33 00 35 00 34 00 64 00 2d 00 34 00 36 00 30 00 61 00 2d 00 39 00 35 00 61 00 64 00 2d 00 62 00 66 00 37 00 38 00 38 00 34 00 65 00 66 00 30 00 39 00 64 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2d8cec74-354d-460a-95ad-bf7884ef09de</Guid>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8130	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8134	2	09 00		success or wait	2	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8138	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 34 00 2d 00 30 00 36 00 2d 00 31 00 39 00 54 00 31 00 32 00 3a 00 33 00 39 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>2024-06-19T12:39:59Z</CreationTime>	success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8236	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8240	2	09 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8242	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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8282	4	0d 00 0a 00		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD31.tmp.WERInternalMetadata.xml	8286	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	6C696C4D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD52.tmp.xml	0	4605	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de\Report.wer	0	2	fd fd		success or wait	1	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de\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	143	6C696C4D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_9fe2b44b45cabaf5e9b80eb2becdba8923fcbda_d2f759d2_2d8cec74-354d-460a-95ad-bf7884ef09de\Report.wer	8498	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 30 00 35 00 30 00 35 00 34 00 37 00 34 00 38 00 37 00	MetadataHash=-1050547487	success or wait	1	6C696C4D	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C69659F	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	ProgramId	unicode	00067e492d768e79731624bcdf2e7615f9180000ffff	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	FileId	unicode	0000d3f5304872ff4b795cde48914fa4d81768abba5d	success or wait	1	6C6B833E	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	LowerCaseLongPath	unicode	c:\users\user\desktop\file.exe	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	LongPathHash	unicode	file.exe|ff8e65d6b06db8e5	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	Name	unicode	file.exe	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	OriginalFileName	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	Publisher	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	Version	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	BinFileVersion	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	BinaryType	unicode	pe32_i386	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	ProductName	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	ProductVersion	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	LinkDate	unicode	06/19/2024 11:40:13	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	BinProductVersion	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	AppxPackageFullName	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	AppxPackageRelativeId	unicode		success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	Size	B	00 F4 06 00 00 00 00 00	success or wait	1	6C6B833E	unknown
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	Language	dword	0	success or wait	1	6C6B833E	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1e5c0749-5a67-aa6e-2372-2b3b37a60da2}\Root\InventoryApplicationFile\file.exe|ff8e65d6b06db8e5	Usn	B	A0 DC 05 07 00 00 00 00	success or wait	1	6C6B833E	unknown

Disassembly

No disassembly