ID: 829686
Sample Name:
Gta_5_Mod_Menu.exe
Cookbook: default.jbs
Time: 21:07:04
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

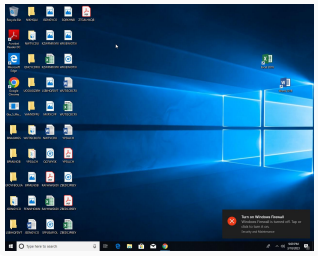
Windows Analysis Report

Gta_5_Mod_Menu.exe

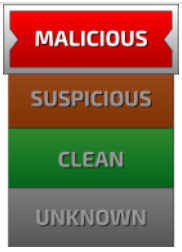
Overview

General Information

Sample Name:	Gta_5_Mod_Menu.exe
Analysis ID:	829686
MD5:	35be3beaaba2…
SHA1:	ce27166d42e8…
SHA256:	1b9192644f191..
Tags:	exe RedLineStealer
Infos:	



Detection



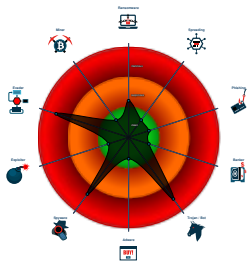
RedLine

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- Gta_5_Mod_Menu.exe (PID: 5924 cmdline: C:\Users\user\Desktop\Gta_5_Mod_Menu.exe MD5: 35BE3BEAABA232F6FDE781242B9C5C4B)
  - conhost.exe (PID: 5992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 3308 cmdline: C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
  - WerFault.exe (PID: 5196 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5924 -s 132 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "82.115.223.46:57672"
  ],
  "Authorization Header": "6ae56e1e5992d446c979c837ad9696f5"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.306737777.0000000000B50000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.295387303.0000000000A52000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.388076605.0000000000402000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 3 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.2.AppLaunch.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd00:$pat14: , CommandLine: • 0x13a96:$v2_1: ListOfProcesses • 0x13875:$v4_3: base64str • 0x143d2:$v4_4: stringKey • 0x1218b:$v4_5: BytesToStringConverted • 0x1139e:$v4_6: FromBase64 • 0x126b4:$v4_8: procName • 0x12e10:$v5_5: FileScanning • 0x12394:$v5_7: RecordHeaderField • 0x1205c:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.3.Gta_5_Mod_Menu.exe.a50000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.Gta_5_Mod_Menu.exe.a50000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd00:$pat14: , CommandLine: • 0x13a96:$v2_1: ListOfProcesses • 0x13875:$v4_3: base64str • 0x143d2:$v4_4: stringKey • 0x1218b:$v4_5: BytesToStringConverted • 0x1139e:$v4_6: FromBase64 • 0x126b4:$v4_8: procName • 0x12e10:$v5_5: FileScanning • 0x12394:$v5_7: RecordHeaderField • 0x1205c:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0.2.Gta_5_Mod_Menu.exe.b40000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 82.115.223.46

Timestamp:	192.168.2.582.115.223.46497025767220432 31 03/18/23-21:08:36.493481
SID:	2043231
Source Port:	49702
Destination Port:	57672
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.5 - Destination IP: 82.115.223.46

Timestamp:	192.168.2.582.115.223.46497025767220432 33 03/18/23-21:08:10.800408
SID:	2043233
Source Port:	49702
Destination Port:	57672
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 82.115.223.46 - Destination IP: 192.168.2.5

Timestamp:	82.115.223.46192.168.2.557672497022043234 03/18/23-21:08:17.271452
SID:	2043234
Source Port:	57672
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

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

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

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

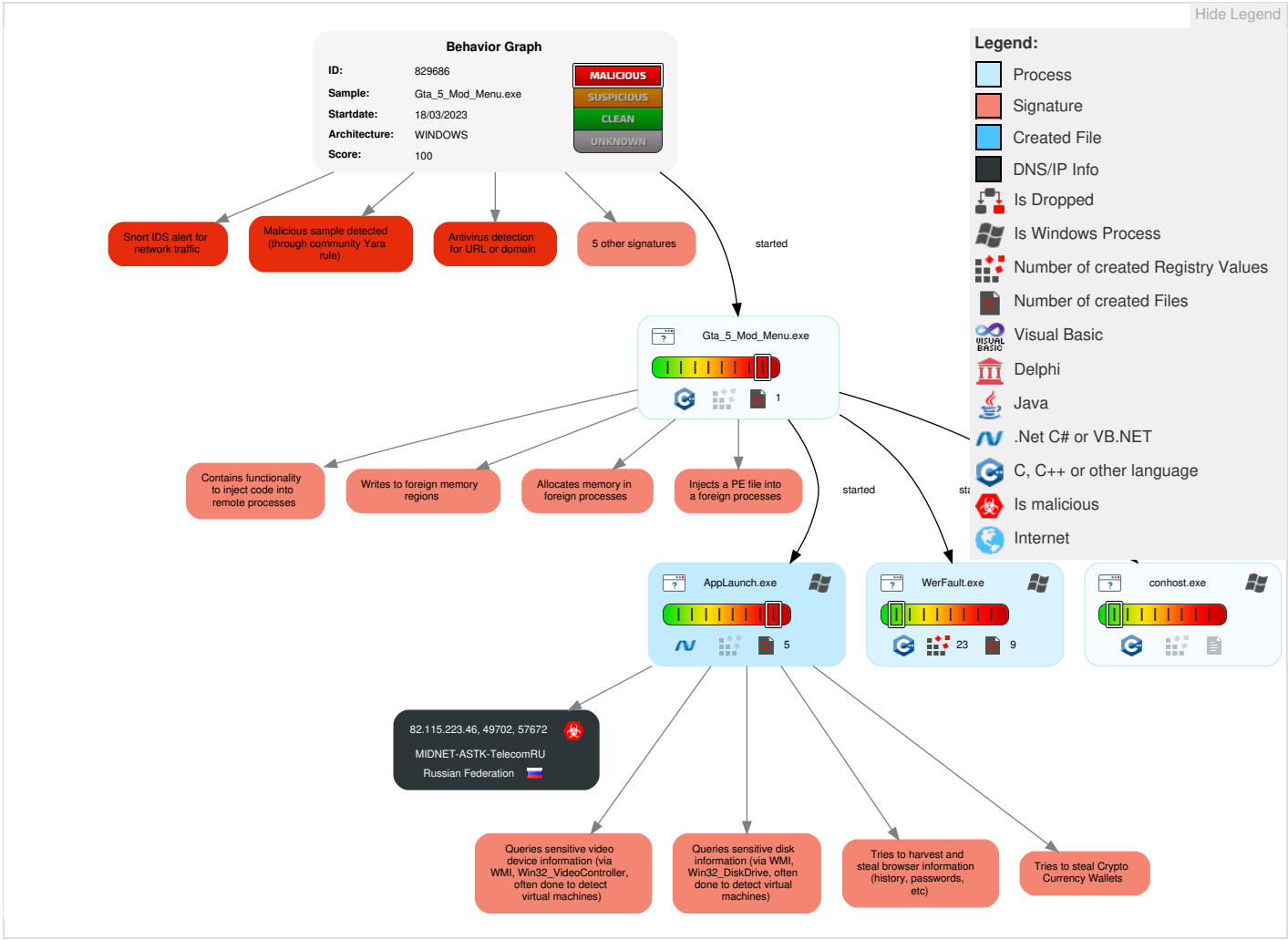
Remote Access Functionality

Yara detected RedLine Stealer

Mitre Att&ck Matrix

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

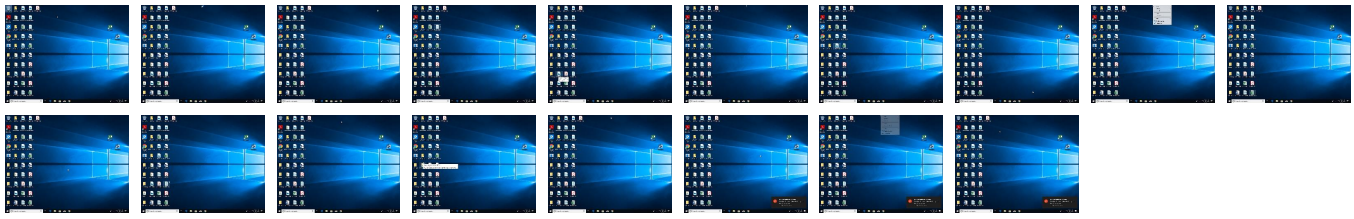
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Gta_5_Mod_Menu.exe	44%	ReversingLabs	Win32.Trojan.RecordBreaker	
Gta_5_Mod_Menu.exe	34%	Virustotal		Browse
Gta_5_Mod_Menu.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
0.3.Gta_5_Mod_Menu.exe.a50000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id19Responseon	100%	URL Reputation	phishing	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultP	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	AppLaunch.exe, 00000002.00000003.3625637 04.000000000820D000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000003.360792439.000000000817100 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000 0000008068000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000003.360792439.0000000008085000.0000 0004.00000800.00020000.00000000.sdmp, Ap pLaunch.exe, 00000002.00000003.362563704 .00000000081F0000.00000004.00000800.0002 0000.00000000.sdmp, AppLaunch.exe, 00000 002.00000003.360792439.0000000008159000. 00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.38992 1530.0000000007394000.00000004.00000800. 00020000.00000000.sdmp, AppLaunch.exe, 0 0000002.00000003.360792439.000000000821E 000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0 00000000712E000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	AppLaunch.exe, 00000002.00000003.3607924 39.0000000008159000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.000000000739400 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000 000000821E000.00000004.00000800.00020000 .00000000.sdmp, AppLaunch.exe, 00000002. 00000002.389921530.000000000712E000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Responseon	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	true	• URL Reputation: phishing	unknown
http://tempuri.org/Entity/Id12Response	AppLaunch.exe, 00000002.00000002.3899215 30.000000000700B000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.0000000006F6F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.0000000006F6F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adobe.c/g	AppLaunch.exe, 00000002.00000003.3800430 88.000000000541C000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000003.379963402.000000000541B00 0.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389461893.000 000000541E000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.0000000006F6F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id7	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.000000000713B00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.0000000006F6F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	AppLaunch.exe, 00000002.00000002.3899215 30.000000000713B000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.0000000006F6F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.000000000700B00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.000000000700B00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000 0000006F6F000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high

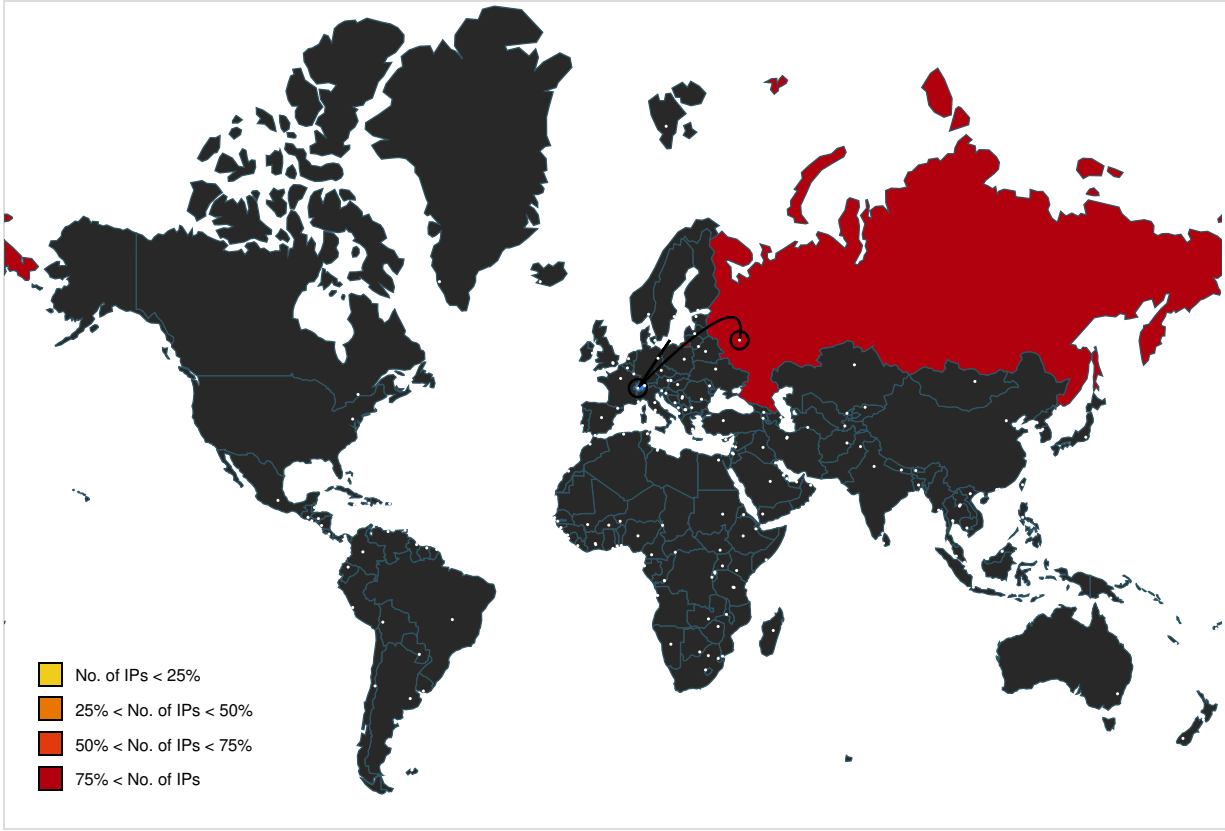
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	Gta_5_Mod_Menu.exe, Gta_5_Mod_Menu.exe, 00000000.00000002.306737777.0000000000B50000.00000004.00000001.01000000.00000003.sdmp, Gta_5_Mod_Menu.exe, 00000000.00000003.295387303.0000000000A52000.00000040.00001000.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.388076605.0000000000402000.00000020.00000400.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000000000713B000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AppLaunch.exe, 00000002.00000003.360792439.000000008159000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000007394000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000000821E000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000000000712E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	AppLaunch.exe, 00000002.00000003.362563704.000000000820D000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000000817000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000008068000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.0000000008085000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.362563704.00000000081F0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.0000000008159000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000007394000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000000821E000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000000000712E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000000000713B000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id13	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.0000000006F6F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00002.00000002.389921530.000000000700B00 0.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000 0000006F6F000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://code.visualstudio.com/0	Gta_5_Mod_Menu.exe	false		high
http://tempuri.org/Entity/Id8Response	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006F6F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	AppLaunch.exe, 00000002.00000002.3899215 30.0000000006EE1000.00000004.00000800.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com?fr=crmas_sfpf	AppLaunch.exe, 00000002.00000003.362563704.000000000820D000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000000817000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000008068000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.0000000008085000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.362563704.00000000081F0000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.0000000008159000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000007394000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000003.360792439.000000000821E000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000000000712E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17Response	AppLaunch.exe, 00000002.00000002.389921530.0000000006EE1000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.000000000713B000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.115.223.46	unknown	Russian Federation		209821	MIDNET-ASTK-TelecomRU	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829686
Start date and time:	2023-03-18 21:07:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Gta_5_Mod_Menu.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/7@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 91.8% (good quality ratio 88.1%) • Quality average: 83.2% • Quality standard deviation: 25.7%

HCA Information:	• Successful, ratio: 97% • 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, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.182.143.212
- Excluded domains from analysis (whitelisted): onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target AppLaunch.exe, PID 3308 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:08:02	API Interceptor	1x Sleep call for process: WerFault.exe modified
21:08:26	API Interceptor	40x Sleep call for process: AppLaunch.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Gta_5_Mod_Menu.e_9a3653fd351b6f67b678151a3e6c91e5fc7_e9b9f6a7_1416ff49\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):	0.8401074420951166
Encrypted:	false

SSDEEP:	96:XCvFDMRMtMzvgMMNwoI7RW6tpXIQcQvc6QcEDMcw3DvMWM6+HbHg/8BRTf3OFL9g:Svy1HBUZMXIjluq/u7sVS274Itt
MD5:	14BAFDB24431A9E6A6E5B01B0C0AB874
SHA1:	476CF6A5F3EFE366D7ABFAF69A887583D59C1EA5
SHA-256:	F1FD1E8515EDB62121A6FD74CBD8D2D5A8997B4AACCF77517665313ED7DA2EA9
SHA-512:	87AA774515F1181DF8017050691A828ED9E474AE0A9C866273C3B930BED73D21248438326D11679F4566569FE9CAFF4D7F545717ABC130290198371366EBCA21
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.3.6.7.2.4.7.9.3.1.9.4.8.0.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.3.6.7.2.4.8.0.4.6.0.1.2.1.7.....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.=.6.3.f.d.7.3.7.e.-.0.b.8.4.-.4.f.e.b.-.b.8.f.d.-.e.f.1.2.b.f.f.6.9.4.3.2.....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.=.d.c.6.4.d.b.f.1.-.c.9.3.1.-.4.e.e.f.-.9.5.8.4.-.d.c.c.0.e.7.4.8.0.4.a.0.....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.=.G.t.a._.5._.M.o.d._.M.e.n.u...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.2.4.-.0.0.0.1.-.0.0.1.9.-.4.7.5.7.-.e.d.6.2.1.8.5.a.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.a.4.7.5.4.c.e.0.7.c.e.a.b.b.3.8.d.b.9.8.4.b.e.8.d.6.9.d.8.1.8.0.0.0.0.1.a.0.8.!.0.0.0.0.c.e.2.7.1.6.6.d.4.2.e.8.1.2.6.a.1.0.3.3.0.f.5.c.b.3.d.7.1.f.5.7.8.f.6.b.7.e.f.5.!.G.t.a._.5._.M.o.d._.M.e.n.u...e.x.e.....T.a.r.g.e.t.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Mar 19 04:07:59 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	40164
Entropy (8bit):	1.884683204606578
Encrypted:	false
SSDEEP:	192:KJuvH2jyaiUO64EKQJXPmajkktidZgU0GGaXFDxzeW+AW:au36ZKGPmawwisUFjCW6
MD5:	60F33FDB80F7869D87D818CFF6623A20
SHA1:	A266BB367029FA2ED5271500F90B7AA3D187BF82
SHA-256:	209EECCD923262FB0079FA01FF80B135F0E63E4591A5625FDB288441DDCD4F02
SHA-512:	83D518A320A99B9F36D3D77867F79320CF98742146AFDADD7E9481EA1A98BBB0B81AA281317A2547C9AB92BA14009769CAC4147250EF03132C4406BD76227F1E
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....d.....&.....T.....8.....T.....U.....B.....8.....GenuineIntelW.....T.....$.....d.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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):	8412
Entropy (8bit):	3.7027281111213677
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipgc6h6YBSvSUngmfzS0Cpra89bn9rsf5dlm:RrlsNipb6h6YB6SUngmfzSvn9wfzo
MD5:	CF45C898B5D086A5808CC687BD543A81
SHA1:	972BF1A9FF72593FA46838FE088B7BE65CBD2DDC
SHA-256:	CBE552C3105BE3870201AD191D58A90C10B1E07987A6B48B2433E9DD435C1F07
SHA-512:	FC9F2E7046F68AC3CF31E1BA0D0AA7AB672D8BE3ED72923A66B503800E5FCC058EDFB3DD61EC7A512783895C54723F67374CECD5FC2823C1283C06E05BD778 96
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2D8.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4734
Entropy (8bit):	4.498836159978724
Encrypted:	false

SSDEEP:	48:cvIwSD8zsMJgtWl9cCtWgc8sqYjV8fm8M4JLPMFk+q8v9PaLoBnizdd:uITfKrCcgrsqYWJzpKlauizdd
MD5:	A9046676DF97E0420E3660EDAED9A7AE
SHA1:	C908E89CB2C4CF1299052B36E10B6E206C80F27A
SHA-256:	601E2BBB1DA03F3020264A49E372F1D8FFFE277305674465F132EBBAAF30A692
SHA-512:	4B2B1FA7C76EC6A4AE78CB957B9367D0B620587D5E409AD91ECC71687D8DD1CF2383EBB68FF2E4E6B69EAA14C9D3CBC3C4F2A13CD088FF0976E3DE50CA6CB135
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1959198" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHK1HjHKg:iqXeqm00YqhQnouOqLqdqNq2qzcGtIxU
MD5:	DCF12DDFCA2FD2701AE5EA0012964E90
SHA1:	AB37B70FB4E34C888BEFFFF54BA5AE34373C816B
SHA-256:	3B28B517A00543FA53ADC147DB9996DF6FF59D002FF65823D5625B44B2D1A406
SHA-512:	5D35EA912835CEB875896F9971225643642245BC6E356AF0D1B370CF4488CE7390D525E526256B9231511DACF4762094D219F20129D96C59778CEF91DDF06538
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.340519568673646
Encrypted:	false
SSDEEP:	12288:ri8GQXFTEDXIRXnMA8adOlZqHcTrlgNvFpe4CRt1TaFNF/z8FDXE05:+8GQXFTEDXIRXnMYR7E
MD5:	5329154E8AA80CB491DA57667FA0A0A9
SHA1:	E63DE714CC83CE5E4CEF69DAEE4E1A20D2DE280C
SHA-256:	35130EC6461CAC33A3A2081535B79C13DDC2BD2CAF16DB72C8F2DDB0F2BB19E9
SHA-512:	653D4DD4C0B968BACD8FFE3F8CF4A6FF3135B7CE3BE33B94D00AA9191293EC928478A2FA78A1E00B1C8908BA1C4A5ACBAD2E3EE8F0BE22D823F4BAB92135D055
Malicious:	false
Preview:	regfY...Y...p.\.,..... ....P.....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.#.c.Z..... ....J.>..... .....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	4.112763655721122
Encrypted:	false
SSDEEP:	384:U5u5+XtnxSC4LK3XJWGV6ypsmcJOosfi4RjYq2xehhfue16abmqDWV:mgqMC4LK3XJWGgyemcJOosfi4RjV2xeL

MD5:	3DDA0D5A6056346F936AE9802CF4DAAA
SHA1:	4BCE21D5649FC72B4CD79D9710FBCC91C284F4FD
SHA-256:	7E7B3E64B4B4504A91F3D3F5EA0517393547564128C36277951A5212487E3E24
SHA-512:	600977B73302178963DBAACDB5F8E99D5647D6737BD25992CFB5F9C72D1CAAEBB6303CFB364D95763058A8B6E5796778F9451B2EC2BE76B1C265E3DDA514A6 5
Malicious:	false
Preview:	regfX...X...p.\..,..... ....P.....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.#.c.Z..... ....J.>HvLE.^.....X....P.....Xjw..A...@..... ...0..hbin.....p.\..,.....nk,..#.c.Z..... .....&...{ad79c032-a2ea-f756-e377-72fb 9332c3ae}.....nk ..#.c.Z..... .....P..... .....Z.....Root.....lf.....Root....nk ..#.c.Z.....}..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.498918006835838
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:	Gta_5_Mod_Menu.exe
File size:	262040
MD5:	35be3beaaba232f6fde781242b9c5c4b
SHA1:	ce27166d42e8126a10330f5cb3d71f578f6b7ef5
SHA256:	1b9192644f1912431596a1c145b7ef462d241551ff9d6782ab1f34def2f373af
SHA512:	9928f1f169d3bcec521c1484533834fc5bbb58fd610d9c067077668c86709a4cafc358a574acd4ae56e97cc9d3a5648c2e1e77c384db5a2fd1ca03fe294aab37
SSDEEP:	3072:9i3kTLikhiGldyOSAmY6AHmSC0xA6t5PHN/rD7FFK/ykXw1wUpZ9jN:M4ukiyn6AH1C0uoU6feiL
TLSH:	A644C538261446E4E4BAD83C2D90B4E070B67533EB87B8FF4E1D3726963119F75A067A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c-.H.C.H.C.H.C.VP.. [.C.VP....C.VP..m.C.o.8.L.C.....K.C.H.B...C.Az..I.C.VP..I.C.Az..I.C.RichH.C.....PE..L...D..d.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40372b
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6414BA44 [Fri Mar 17 19:06:44 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	df35d969e1568731b4c070bee6bd7122

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	CN=Microsoft Code Signing PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 5/12/2022 1:46:02 PM 5/11/2023 1:46:02 PM
Subject Chain	• CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	D03E1ED3E72F64CC6C5A636BE32C29AD
Thumbprint SHA-1:	97221B97098F37A135DCC212E2B41E452BCE51F2
Thumbprint SHA-256:	AAE358FD90D5500110EE8BF3BD2C668F834559710DA7D75C266018BB9506F2F6
Serial:	33000002CDF364BFF8D44C5D510000000002CD

Entrypoint Preview

Instruction
call 00007FE5487725C1h
jmp 00007FE54876FFB9h
mov edi, edi
push esi
push 00000001h
push 0043B9E4h
mov esi, ecx
call 00007FE548772641h
mov dword ptr [esi], 0040D8D4h
mov eax, esi
pop esi
ret
mov dword ptr [ecx], 0040D8D4h
jmp 00007FE5487726A6h
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
mov dword ptr [esi], 0040D8D4h
call 00007FE548772693h
test byte ptr [ebp+08h], 00000001h
je 00007FE548770119h
push esi
call 00007FE548770FDDh
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FE548772612h
mov dword ptr [esi], 0040D8D4h
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0Ch
jmp 00007FE54877011Fh

Instruction
push dword ptr [ebp+08h]
call 00007FE54877292Bh
pop ecx
test eax, eax
je 00007FE548770121h
push dword ptr [ebp+08h]
call 00007FE548772845h
pop ecx
test eax, eax
je 00007FE5487700F8h
leave
ret
test byte ptr [0043CA20h], 00000001h
mov esi, 0043CA14h
jne 00007FE54877012Bh
or dword ptr [0043CA20h], 01h
mov ecx, esi
call 00007FE548770069h
push 0040C9DBh
call 00007FE5487727B2h
pop ecx
push esi
lea ecx, dword ptr [ebp-0Ch]
call 00007FE5487800A2h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf5f4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x640	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3d800	0x2798	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3f000	0xd48	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0x10c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb9ef	0xba00	False	0.5593287970430108	Matlab v4 mat-file (little endian) \354\010VW\307E\374, numeric, rows 0, columns 0	6.74235183795128	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x2c1a	0x2e00	False	0.454398777173913	data	5.8872406447459396	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x10000	0x2d5fc	0x2ca00	False	0.5094318977591037	data	6.047903459156929	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3e000	0x640	0x800	False	0.353515625	data	3.288698491356012	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3f000	0x1940	0x1a00	False	0.4343449519230769	data	4.294613327745058	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3e200	0x43c	data	English	United States
RT_MANIFEST	0x3e0a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.582.115.223.46 49702576722043231 03/18/23-21:08:36.493481	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49702	57672	192.168.2.5	82.115.223.46
192.168.2.582.115.223.46 49702576722043233 03/18/23-21:08:10.800408	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49702	57672	192.168.2.5	82.115.223.46
82.115.223.46192.168.2.5 57672497022043234 03/18/23-21:08:17.271452	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	57672	49702	82.115.223.46	192.168.2.5

TCP Packets

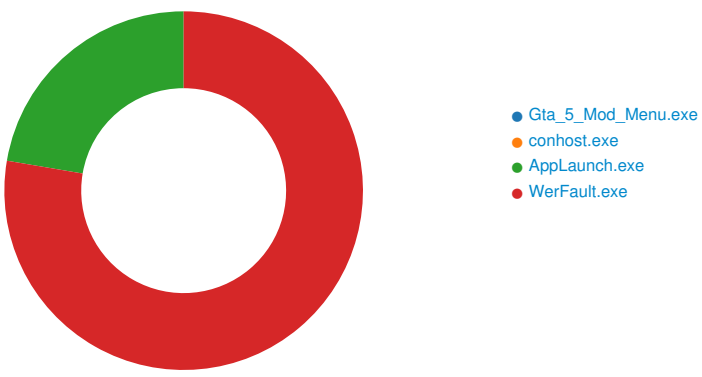
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 21:08:10.409373045 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:10.450601101 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:10.450761080 CET	49702	57672	192.168.2.5	82.115.223.46

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 21:08:10.800407887 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:10.869298935 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:10.924046040 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:16.963551998 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:17.004424095 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:17.127687931 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:17.271451950 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:17.271528959 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:24.290375948 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:24.335110903 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:24.335145950 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:24.335171938 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:24.335274935 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:24.378298998 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:25.688733101 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:25.730191946 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:25.776598930 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:29.940876007 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:29.982038975 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.011507034 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.051670074 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.097543955 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.220794916 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.260781050 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.261393070 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.316317081 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.426809072 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.467431068 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.519529104 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.578352928 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.621465921 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.626569986 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.667372942 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.669123888 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.719435930 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.769529104 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.804426908 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.844351053 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.844722986 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.846446991 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.886729956 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:30.930843115 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:30.972645998 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.839720011 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.879996061 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.880155087 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.880271912 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.880367994 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.880403042 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.880496979 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.880831957 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.880932093 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.919970036 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.920170069 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.920243025 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.920391083 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.920597076 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.920741081 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.921220064 CET	57672	49702	82.115.223.46	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 21:08:31.921241999 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.921344042 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.921842098 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.922189951 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.922471046 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.923208952 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.923357964 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.960102081 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.960396051 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.960792065 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.961306095 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.961800098 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.962002993 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.962584019 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.963124037 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.963125944 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.963265896 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.963465929 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.963587046 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.963939905 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.964416981 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.964668989 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.964757919 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:31.965110064 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:31.965209007 CET	49702	57672	192.168.2.5	82.115.223.46
Mar 18, 2023 21:08:32.004133940 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.004273891 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.004314899 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.005147934 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.005208015 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.005717039 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.006462097 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.006546974 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.007570982 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.008021116 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.008088112 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.008769989 CET	57672	49702	82.115.223.46	192.168.2.5
Mar 18, 2023 21:08:32.009454966 CET	57672	49702	82.115.223.46	192.168.2.5

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Gta_5_Mod_Menu.exe PID: **5924**, Parent PID: **3324**

General

Target ID:	0
Start time:	21:07:56
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\Gta_5_Mod_Menu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Gta_5_Mod_Menu.exe
Imagebase:	0xb40000
File size:	262040 bytes
MD5 hash:	35BE3BEAABA232F6FDE781242B9C5C4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.306737777.0000000000B50000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.295387303.0000000000A52000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5992**, Parent PID: **5924**

General

Target ID:	1
Start time:	21:07:57
Start date:	18/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **3308**, Parent PID: **5924**

General

Target ID:	2
Start time:	21:07:57
Start date:	18/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true

Commandline:	C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe
Imagebase:	0x1190000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.388076605.0000000000402000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.389921530.0000000006F6F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.389921530.000000000700B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7107BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7107BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	0	2843	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	7253C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	151	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	14	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	82	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	164	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	702	end of file	2	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	71071B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	71071B4F	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.docx	unknown	4096	success or wait	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\JSDNGYCOWY.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	1022	end of file	1	71071B4F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: WerFault.exe PID: **5196**, Parent PID: **5924**

General

Target ID:	5
Start time:	21:07:58
Start date:	18/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5924 -s 132
Imagebase:	0x360000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	69B61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2D8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2D8.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Gta_5_Mod_Menu.e_9a3653fd351b6f67b678151a3e6c91e5fc7_e9b9f6a7_1416ff49	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	69B5497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Gta_5_Mod_Menu.e_9a3653fd351b6f67b678151a3e6c91e5fc7_e9b9f6a7_1416ff49\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	69B5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2D8.tmp	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2D8.tmp.xml	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2E5.tmp.csv	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF509.tmp.txt	success or wait	1	69B5497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd fd 16 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	5944	6	00 00 00 00 00 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 38 17 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 24 17 00 00 fd fd 16 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UB8GenuineIntelWT$d0Pacific Standard TimePacific Daylight Time	success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	6888	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 73 fd fd 00 fd fd fd 00 00 00 34 02 51 78 fd 00 00 00 00 00 73 fd fd 00 fd fd fd 00 23 00 00 00 46 02 01 00 fd fd 4f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++s4Qxs#FO+	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	1620	168	1c 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1a 00 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	9752	20	0d 00 00 00 58 6a 75 00 00 00 00 00 04 00 00 00 fd 26 00 00	Xju&	success or wait	13	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	9964	4	14 12 09 77	w	success or wait	12	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	31140	1436	fd fd 0f 77 fd fd 0d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 6f 00 fd fd 6f 00 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 fd 27 00 00 fd 27 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 27 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 6e 75 00 00 00 00 00 00 00 00 00 00 00 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 fd 6f 76 00 00 00 00 00 00 00 00 00 58 6a 75 00 00 20 27 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 54 22 27 00 fd fd fd 00 fd 6e 75 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwoo@w@w'"nuovXju 'T"'nu	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	1788	4	03 00 00 00		success or wait	3	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	7604	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 51 78 fd 00 00 00 00 00 fd fd 4f 00 fd fd 0f 77 23 00 00 00 16 02 00 00 30 fd 4f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++QxOw#0O+	success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	1888	48	fd 0a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 27 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 05 00 00 68 74 00 00 fd 02 00 00 4c 23 00 00	'<htL#	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	1948	4	1f 00 00 00		success or wait	31	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	5950	42	24 00 00 00 47 00 74 00 61 00 5f 00 35 00 5f 00 4d 00 6f 00 64 00 5f 00 4d 00 65 00 6e 00 75 00 2e 00 65 00 78 00 65 00 00 00	$Gta_5_Mod_Menu.exe	success or wait	31	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	5192	752	00 00 fd 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1a 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 15 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 45 fd 03 00 00 00 00 00 7e fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 34 1b 00 00 00 00 00 4c fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 03 05 00 00 00 00	v`A!-aBB? #@AZbpFE~4L@	success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	32576	7588	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF111.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 18 0d 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 18 26 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 15 00 00 fd 00 00 15 00 00 00 fd 01 00 00 fd 14 00 00 16 00 00 00 fd 00 00 00 fd 16 00 00	&T8T	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5924</Pid>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1002	82	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 47 00 74 00 61 00 5f 00 35 00 5f 00 4d 00 6f 00 64 00 5f 00 4d 00 65 00 6e 00 75 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>Gta_5_Mod_Menu.exe</ImageName>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1084	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1088	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1092	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>000000</CmdLineSignature>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1182	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1186	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1190	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 37 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2705</Uptime>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1232	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1236	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1240	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1322	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1326	2	09 00		success or wait	2	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1330	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1382	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1386	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1390	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1434	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1438	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1444	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 31 00 36 00 31 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>82161664</PeakVirtualSize>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1530	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1534	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1540	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 30 00 34 00 36 00 31 00 38 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>80461824</VirtualSize>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1610	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1614	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1620	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 38 00 32 00 36 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>1826</PageFaultCount>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1694	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1698	2	09 00		success or wait	3	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1704	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 36 00 30 00 38 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>6860800</PeakWorkingSetSize>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1810	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 31 00 35 00 37 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6815744</WorkingSetSize>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1890	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1894	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	1900	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>154736</QuotaPeakPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2014	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2018	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2024	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 33 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>153768</QuotaPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2122	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2126	2	09 00		success or wait	3	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2132	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>20168</QuotaPeakNonPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2256	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2260	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2266	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 39 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19896</QuotaNonPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2374	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2378	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2384	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 31 00 37 00 39 00 32 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>1617920</PagefileUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2460	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2464	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2470	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 31 00 34 00 35 00 32 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>18145 28</PeakPagefileUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2572	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 31 00 37 00 39 00 32 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>1617920</PrivateUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2644	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2648	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2652	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2698	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2702	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2706	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2736	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2740	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2746	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2786	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2790	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2798	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2828	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2832	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2840	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2910	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2914	2	09 00		success or wait	4	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	2922	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3012	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3016	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3024	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 34 00 33 00 34 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5343409</Uptime>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3072	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3076	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3084	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3162	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3166	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3174	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3238	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3282	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3286	2	09 00		success or wait	5	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3296	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3386	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3390	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3400	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3474	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3478	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3488	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 32 00 33 00 36 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>62367</PageFaultCount>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3578	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 35 00 36 00 30 00 37 00 39 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>125607936</PeakWorkingSetSize>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3692	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 35 00 32 00 36 00 33 00 38 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>125263872</WorkingSetSize>	success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3776	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3780	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3790	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 38 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11800 56</QuotaPeakPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	3920	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 33 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1143232</ QuotaPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4020	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4024	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4034	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 39 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4158	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4162	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4172	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 33 00 37 00 34 00 34 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>83744< /QuotaNonPagedPoolUsage>	success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4280	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4284	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4294	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 36 00 35 00 39 00 36 00 30 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>46596096</PagefileUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4372	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4376	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4386	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 37 00 35 00 34 00 32 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>47542272</PeakPagefileUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4480	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4484	2	09 00		success or wait	5	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4494	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 36 00 35 00 39 00 36 00 30 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>46596096</PrivateUsage>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4568	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4572	2	09 00		success or wait	4	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4580	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4636	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4678	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4682	2	09 00		success or wait	2	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4686	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4724	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4766	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4770	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4772	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4810	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4814	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4818	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	9	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	18	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	4878	86	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 47 00 74 00 61 00 5f 00 35 00 5f 00 4d 00 6f 00 64 00 5f 00 4d 00 65 00 6e 00 75 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>Gta_5_Mod_Menu.exe</Parameter0>	success or wait	9	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5616	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5656	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5660	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5662	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	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5700	4	0d 00 0a 00		success or wait	6	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5704	2	09 00		success or wait	12	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	5708	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6268	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6308	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6312	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6314	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6352	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6356	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6360	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6454	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6458	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6462	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 63 00 65 00 79 00 73 00 78 00 64 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ceysxd, Inc.</SystemManufacturer>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6568	4	0d 00 0a 00		success or wait	1	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6572	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6576	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 65 00 79 00 73 00 78 00 64 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ceysxd7,1</SystemProductName>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6672	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6676	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6680	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6800	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6804	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6808	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 35 00 31 00 38 00 36 00 33 00 39 00 37 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1635186397</OSInstallDate>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6890	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6894	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	6898	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	2	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7008	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7076	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7080	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7082	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7128	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7162	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7166	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7170	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7272	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7308	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7312	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7314	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7338	4	0d 00 0a 00		success or wait	3	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7342	2	09 00		success or wait	6	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7346	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7590	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7594	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7596	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7622	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7626	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7628	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 33 00 2d 00 31 00 39 00 54 00 30 00 34 00 3a 00 30 00 37 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-03-19T04:07:59Z">	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7728	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7732	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7736	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 33 00 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 39 00 32 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 39 00 32 00 31 00 22 00 20 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="302" PID="5924" UptimeMS="921" TimeSinceCreationMS="921" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7994	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	7998	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8002	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	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8022	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8026	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8028	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8066	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8070	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8072	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8110	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8114	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8118	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 33 00 66 00 64 00 37 00 33 00 37 00 65 00 2d 00 30 00 62 00 38 00 34 00 2d 00 34 00 66 00 65 00 62 00 2d 00 62 00 38 00 66 00 64 00 2d 00 65 00 66 00 31 00 32 00 62 00 66 00 66 00 36 00 39 00 34 00 33 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>63fd737e-0b84-4feb-b8fd-ef12bff69432</Guid>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8216	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8220	2	09 00		success or wait	2	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8224	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 33 00 2d 00 31 00 39 00 54 00 30 00 34 00 3a 00 30 00 37 00 3a 00 35 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-03-19T04:07:59Z</CreationTime>	success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8322	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8326	2	09 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8328	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8368	4	0d 00 0a 00		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF269.tmp.WERInternalMetadata.xml	8372	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	69B5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2D8.tmp.xml	0	4734	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	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Gta_5_Mod_Menu.e_9a3653fd351b6f67b678151a3e6c91e5fc7_e9b9f6a7_1416ff49\Report.wer	0	2	fd fd		success or wait	1	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Gta_5_Mod_Menu.e_9a3653fd351b6f67b678151a3e6c91e5fc7_e9b9f6a7_1416ff49\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	158	69B5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Gta_5_Mod_Menu.e_9a3653fd351b6f67b678151a3e6c91e5fc7_e9b9f6a7_1416ff49\Report.wer	10356	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 33 00 34 00 39 00 39 00 34 00 36 00 36 00 32 00 30 00	MetadataHash=349946620	success or wait	1	69B5497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	success or wait	1	69B736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69B71FB2	RegCreateKeyExW
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69B543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	ProgramId	unicode	00064a4754ce07ceabb38db984be8d69d81800001a08	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	FileId	unicode	0000ce27166d42e8126a10330f5cb3d71f578f6b7ef5	success or wait	1	69B736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	LowerCaseLongPath	unicode	c:\users\user\desktop\gta_5_mod_menu.exe	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	LongPathHash	unicode	gta_5_mod_menu.e|71a7622c	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	Name	unicode	gta_5_mod_menu.exe	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	Publisher	unicode	oars	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	Version	unicode	4.33.138.2	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	BinFileVersion	unicode	4.33.138.2	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	BinaryType	unicode	pe32_i386	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	ProductName	unicode	craves whirred	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	ProductVersion	unicode	4.33.138.2	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	LinkDate	unicode	03/17/2023 19:06:44	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	BinProductVersion	unicode	4.33.138.2	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	Size	B	98 FF 03 00 00 00 00 00	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	Language	dword	2074	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	IsPeFile	dword	1	success or wait	1	69B736BF	unknown
\REGISTRY\A\{6b71d3f5-24bd-1e26-b17e-92529311131a}\Root\InventoryApplicationFile\gta_5_mod_menu.e|71a7622c	IsOsComponent	dword	0	success or wait	1	69B736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 85 82 B3 00 02 00 00 00 08 00 00 00 85 82 B3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	69B71FE8	RegSetValueExW

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

Disassembly

No disassembly