ID: 490250
Sample Name:
Z5kAk5QCIB.exe
Cookbook: default.jbs
Time: 10:11:52
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

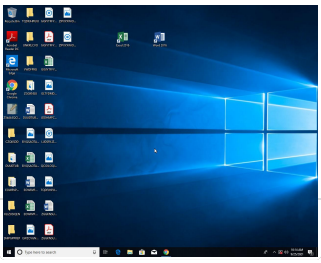
Windows Analysis Report Z5kAk5QCIB.exe

Overview

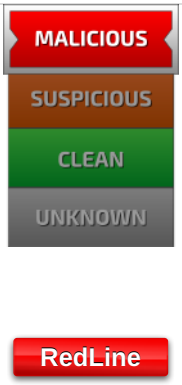
General Information

Sample Name:	Z5kAk5QCIB.exe
Analysis ID:	490250
MD5:	6b372844c175ae..
SHA1:	d2dba224689f9c3.
SHA256:	8b0d5e431a0e9c..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

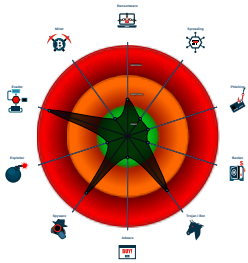


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Wallets
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- Z5kAk5QCIB.exe (PID: 4140 cmdline: 'C:\Users\user\Desktop\Z5kAk5QCIB.exe' MD5: 6B372844C175AEC62ACC6CC18E1F8006)
  - conhost.exe (PID: 712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "45.9.20.20:13441"
  ],
  "Bot Id": "UTS"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.313769707.0000000002EAB000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.391337431.0000000004AD0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.393187019.0000000005D65000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.390510548.00000000048A0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.391542368.0000000004B2C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Z5kAk5QCIB.exe.48a0000.3.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.Z5kAk5QCIB.exe.48a0ee8.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.Z5kAk5QCIB.exe.48a0000.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.Z5kAk5QCIB.exe.4ad0000.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.Z5kAk5QCIB.exe.4b6d876.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

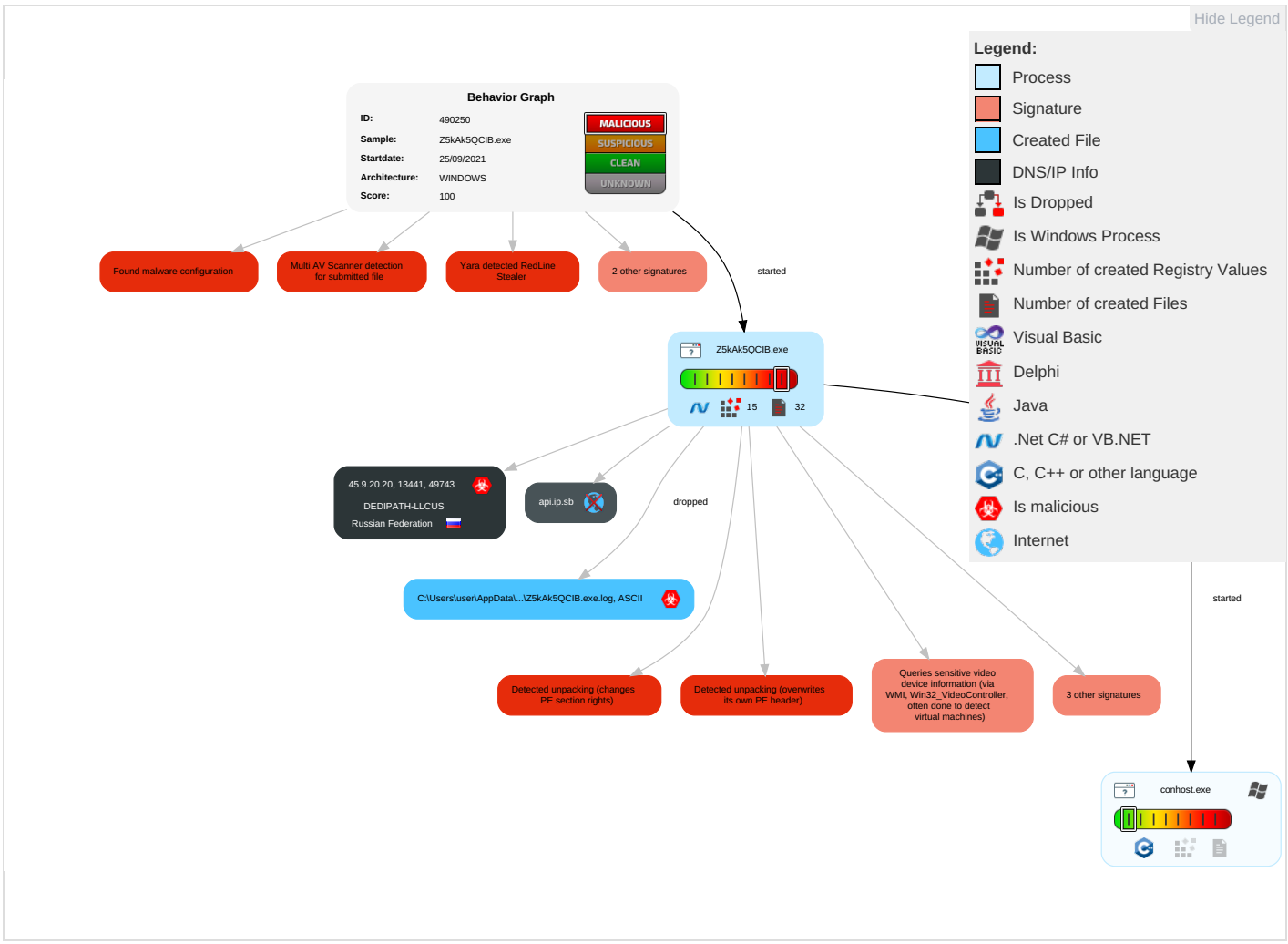
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comn
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 6 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	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	Software Packing 2	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

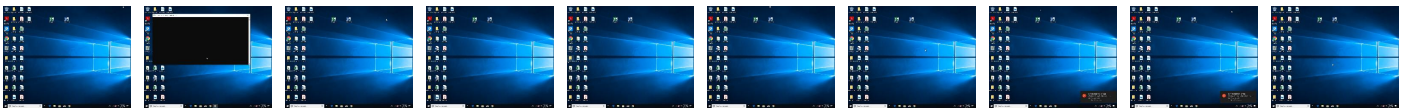
Behavior Graph



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
Z5kAk5QCIB.exe	33%	Virustotal		Browse
Z5kAk5QCIB.exe	52%	ReversingLabs	Win32.Trojan.Glupteba	
Z5kAk5QCIB.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api.ip.sb	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Endpoint/PartInstalledSoftwares	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Endpoint/PartNordVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscord	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledBrowsersResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartColdWalletsResponse	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/PartInstalledSoftwaresResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartProtonVPNResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscordResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartFtpConnectionsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartOpenVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartOpenVPNResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartProtonVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartHardwaresResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartTelegramFilesResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/Init	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ip.sb	unknown	unknown	false	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.9.20.20	unknown	Russian Federation		35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490250
Start date:	25.09.2021
Start time:	10:11:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Z5kAk5QCIB.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@2/27@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10% (good quality ratio 9.7%) • Quality average: 85% • Quality standard deviation: 23.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:13:27	API Interceptor	61x Sleep call for process: Z5kAk5QCIB.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.9.20.20	5DxtZ6xMrB.exe	Get hash	malicious	Browse	
	qefGuXETjf.exe	Get hash	malicious	Browse	
	aVfFzvm8iR.exe	Get hash	malicious	Browse	
	6UclBifP3f.exe	Get hash	malicious	Browse	
	jroJZULz8w.exe	Get hash	malicious	Browse	
	976y4GH2rY.exe	Get hash	malicious	Browse	
	3zb0mumThM.exe	Get hash	malicious	Browse	
	Z1LjJ5odpI.exe	Get hash	malicious	Browse	
	JGam14245S.exe	Get hash	malicious	Browse	
	rj6qxIrooh.exe	Get hash	malicious	Browse	
	EZpSqv83eJ.exe	Get hash	malicious	Browse	
	SCym9cuPKq.exe	Get hash	malicious	Browse	
	yqxz73qFDp.exe	Get hash	malicious	Browse	
	W6fjwqXDfO.exe	Get hash	malicious	Browse	
	NcX0SHPIGm.exe	Get hash	malicious	Browse	
	eucPRBGIG4.exe	Get hash	malicious	Browse	
	n2T78kB7vE.exe	Get hash	malicious	Browse	
	6QnP1PXwHi.exe	Get hash	malicious	Browse	
	DUIuBOErSU.exe	Get hash	malicious	Browse	
	dVJXoBazmx.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	5DxtZ6xMrB.exe	Get hash	malicious	Browse	• 45.9.20.20
	qefGuXETjf.exe	Get hash	malicious	Browse	• 45.9.20.20
	aVfFzvm8iR.exe	Get hash	malicious	Browse	• 45.9.20.20
	6UclBifP3f.exe	Get hash	malicious	Browse	• 45.9.20.20
	jroJZULz8w.exe	Get hash	malicious	Browse	• 45.9.20.20
	976y4GH2rY.exe	Get hash	malicious	Browse	• 45.9.20.20
	3zb0mumThM.exe	Get hash	malicious	Browse	• 45.9.20.20
	Z1LjJ5odpI.exe	Get hash	malicious	Browse	• 45.9.20.20
	JGam14245S.exe	Get hash	malicious	Browse	• 45.9.20.20
	rj6qxIrooh.exe	Get hash	malicious	Browse	• 45.9.20.20
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 45.133.1.182
	EZpSqv83eJ.exe	Get hash	malicious	Browse	• 45.9.20.20
	SCym9cuPKq.exe	Get hash	malicious	Browse	• 45.9.20.20
	yqxz73qFDp.exe	Get hash	malicious	Browse	• 45.9.20.20
	W6fjwqXDfO.exe	Get hash	malicious	Browse	• 45.9.20.20
	NcX0SHPIGm.exe	Get hash	malicious	Browse	• 45.9.20.20
	Consignment Documents.exe	Get hash	malicious	Browse	• 45.144.225.194
	Shipping Declaration.exe	Get hash	malicious	Browse	• 45.144.225.112
	eucPRBGIG4.exe	Get hash	malicious	Browse	• 45.9.20.20
	n2T78kB7vE.exe	Get hash	malicious	Browse	• 45.9.20.20

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Z5kAk5QCIB.exe.log	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKYHZHAHxLHG1qHu:Pqaq5qXAqLqdqUqzcGYqhQnoPtIxHbqS
MD5:	66D7E07C835F707963009A207CDC770B
SHA1:	8D3D65EA8FD18976FF325E0812F0DD8B6C12F275
SHA-256:	7840FE961948856C25B191A6013E8694CC8E0B80F7B8A6A474C45EB0FB53A336
SHA-512:	F36B511EA43599DB92751D8873EE429D8B5D342BA14E8C9EEC9250A21C2373B2EF10E4E6C8372B8011023FAE8B76E04CF09557186CB6D5B28C44408F661C7955
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b

C:\Users\user\AppData\Local\Temp\tmp1E2C.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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

C:\Users\user\AppData\Local\Temp\tmp1E2C.tmp	
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp1E2D.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp1E2E.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp1E2F.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp3943.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701195573484743
Encrypted:	false
SSDEEP:	24:CXuIDWqLgX6vdVaxL46BNaYMbtbF+qEBHi7z/dd0Vc/6cUmeDs:ODHgX6vd0l4gnMbtbF+qEMPdNiTmcs
MD5:	2530C45A92F347020337052A8A7D7B00
SHA1:	7EB2D17587824A2ED8BA10D7C7B05E2180120498
SHA-256:	8BEAEA56B1D06BFFFE6142E95BC808FD28015E6A3FF32BC2FAC4C5A7552FC853
SHA-512:	78F4D4E93139D099D59F17867A6BB87A7DB92E1637A520B522A32DF14D18A39602F1C255C64C4C406BA45138294D9467850FEEA90C199D3434D60AE1C7F6B4DA
Malicious:	false
Preview:	DUUDTUBZFWQODSNPWYYAIDZFECIUBQYLVGHZRZFDGGWVZPGQSHTPZANMRMNDUZLXCVYYIRRTMYEOTHOFJLCKQKOCQKNMRKZTHKIIPBKXIKLDAZ FJGRVUHMDDXAMADOCGROYYDTNZZUEROBUVEGQEAZOMYVDGVHXUWCBVRBLFLWITRUFMXJJLQTZTWLOSFUMQDKRZDXVRLBYBKLXGLTGADROPECYT RYJQJWZDWJQHGRYFIQLJDBJUFPEPZLWGXGGDQGOLJCVZAPHJZOSIZQHISQFRJJGEZIJEFACYWHJRHAADQBMDQFJAGFBEZNQNGWDHSAAXOAEHIE HTAEPMOFJSOCRPTEUZGGSVYGVNUAYJPFNXFSYEEMDNDGDUBNXUOHVEJQBDRGSCASTDANAAFPQYQEHHTAOTYKYJJYXDZMUTBXBCIFNYSYWNMYAE EUEIGDANIBIJWTMCMGVDPOCAVEJZDTVMKOQPOOOKMLFWWMOASXZUZVHWZKPBVANJIBBDPCEKXDPEFNTXPTFJRBFUPHQCKMDMMXQPDZLJPURSOL PQREZLEFYXCGNKSFQRMLKDMGSNURCWGNTDQUIOYBPNJAYWOVTXRGROGVHNGIEDBYKUHNRBBDKYQXANPQWPKEOHDUBNRSQPALMLJE QFMXCQMEOAKBRREEJTYCHGUEGBGPJLGWRCLYLAKRESHJPMPCUHRFXHVUIQCQZYDTCNRGWVTYBMIILXIIIOGMHAQBLHFXCLTIKGXWDVRGSSRDNC YOVCLTUUEWRIDEOSWWZKTQLGLSIFPVAFJDGWVZYJUOVTMGGZMWUYOQYCLDNLMKWCJBKOXTWTPCMMIEYMISQTQCKMPNWJVAXPFISOGTRIMGKBHK EJOEDYIGOBOPVFADMXZUZQZVMUDYSPUHDXFZMAVPGIHURQNBZXXDWPSHUEZEFABRCKBUQLCPYBNGKJCWBTBSWMABCFIYQJOHFJJEPNNMRWWMNL OTWSMOXCILCCNICPDFTO

C:\Users\user\AppData\Local\Temp\tmp3944.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.692990330209164
Encrypted:	false
SSDEEP:	24:NCzz4hMQMxH70HULgnraTryj1S0KEX64u+O572j79DwzpnQf8A:axH70cauYS0k4u+O125wtnm8A
MD5:	DD71B9C0322AD45992E56A9BCE43FE82
SHA1:	60945B6BC3027451A2E1CFA29D263A994F50E91A
SHA-256:	19AC62FD471E562088365029F7B0672623511CF3E58F2EF6DE1A15C14A2E94E7
SHA-512:	86EA2B42FEB542977FCF534B4708F7A07E09F4ACC413307E660B905408BC4AA9E26C50E907FA02379EA3EBFD18C532CC9DC269B6EA5994E3290082E429CAAE0 3
Malicious:	false
Preview:	EOWRVPQCCSGUYRPSSKREBPXVQXUWKHGDIJHLBLYMXTIUESLNTSFMRJGDSQHOWECQAJMENKQNNWPVETUPWMXJTCUIAKPCZEENXVLTKYPKROZPDE BFNAJOVCNEXQJFUHQCMLNHGMRJJIPLOMWFWJKKXSTRHWFVLVQPEMFBLDTSCCSXADJIIDQIYCEGSDEDZDWUEJLTYJHMYEHHMBFZCRDHXZVPESWN DGUEFQZTJFSJVKZMWREMIZGAIZANQJKWWXITTXHDQDZOEOGKCEMDUUBDTMNWBRSOWEKQXQDCYJXERQRAMVQCWCTYJPEAJUAWNBRQ WGFJAHXJJFRYTZMSGCREPRECKHXXMJGSQEKUCUNCWUAAPBWQVSMWCJGYSLPHJJHJGXSMNLNICJMSGSWRKARHMQXLYSAOPDAPXSMO RZLUWYOQTJQNKSCAJWRUEYRFPNOVSMNYRKMTSGRIFLOAJUGJYDTLINOTCEADKRENVYNODFSIJGSDCICIDXZTLLSKKJQSOHYTZRBSHPHXWZOOSK QIRSGPTAOQPBVJAMXOGPYNJMJXAKCTMRRTFCBPOAMNJORWRNZOGZMNBVCCZYQPOQOUXBGKNLFSQWAWEREFQBRDLTVHEFNRUSOARH JPRECDRMPANZRBGCANIUWEBUDVWLYHFTPGBHSZBZBEFUWFHUZPJOVMHGSINZWDUKWPGMGSNSSJNOMETOCJILXRQRGZQFAJCWYQEENIZIMHRBTZ UYEOKCQXYLWCKFHOHCOVRVPNTEUARVJEFALBUVYXIYZRMGJWZNYNLPYHZSSCODVXZBIWXIOAVMGMPKCPYIFZIKWRIHNIYASXZLMOLNZOMMYUSC RZBCXRANWWODLPHCXXDPLNYLMHYIUYZJWQLECFNXQEERYDVDBPXOLGZLZQCVYUYKFZGKXWVDQANPXQYAATYFJALGENVLDMHDASWKNNXODUHLXY GCBUKEFWISCCUWXNUNETWMTQHQDJMAXNPFPLMPQO

C:\Users\user\AppData\Local\Temp\tmp3945.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6959554225029665
Encrypted:	false
SSDEEP:	24:TifvYKkubZMu3HGRW2lJUao1nH5o4WGAZ46:rKkmZMuklJUj+GAZ46
MD5:	DCABA2748DFEAEF0BFBC56FD9F79315C
SHA1:	B87FBA690A774893B22B9F611DFDCB5CDC520269
SHA-256:	86DF5957E0CD2EBDFC2FF8C2F05569BA71462149042DF57ECE5E8228E3BC5DDD
SHA-512:	65F10692D0AE5CBAADDB03E89D6CD1D3486429906437A17C2B1157BEDB069202B1DC52A4E864AA8F90B8CBD171FD2A3E150185BF7DFF81540E209B6A8F8829I 3
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp3945.tmp	
Preview:	ZGGKNSUKOPMPPNHVZHJQGVEFQIYKECDTBUUNZDYNGQNIRYRWHUTXXPSHQTZPTZVHQXNNQJMVUKUOXVGORIAYJGXFFBGSTKCIJZKEQXQQIVFFMJ LOMJSXIEOLRGDCSILZBJCYZNNVATINEQDJPDYKYEGAQWQMEKFVPOYVPNSSIUTCUVWRTSGVMOYKONZJJHVYYHDVZQPBVLAEYYFULQVIAJCQYCDC EGDPRRLXXZXFIPXZYSZYOHEAPCISCQQIAXVPAQUVHGATHPNBNNZVCLFBZBDBZXOQODZLPUONDHVUIQLSZFYHOZHZHEGULYTEVGGLQVDEJVLJEV PQFWMTICLCXTQWMOFFAXIMODRSEVRDYZWTZFYKVZAJEAQBNILURHKTJBNMYKYFSYGEEBYTRKZAHNYHNKUVIQXUDTDSCKKVFAHEOCHUYENGZNJL YIKKSHPNCIQVEDXXJBQWLPTRWDPYUIEDKEYQXNAFVHZZHVLORWXSFDRTMIHTRSJAHAAHMDOMCQGDKDFHBNGVZQTTCSWSPIHCTQXSLLYZTFMEMA CZONDWHGUSVOCWSBRSQZPAKSJHSWPMXYNSVNZCBVQSSDMAXHBCCABCBJMXUBBMSGLUNDNJSGZUMDVFIJNOELGIFULZKPJDVNZQPDOWCXYQGTVJ KDHOFHYVKNSZDNMILUISTCTZRFSEWRMDZLOBGFMXNVDCJYYLJUDJGSTSUEEGOSENKRNGXAGHHNOGGDSDRGIFROBPWJOCJPXDATRXEPUOWMBLLO QTSWYHGAJBORDMNUEAHWTKUYXIIPMYCMRMTPBVKTCXSHVYJOWCUSTTUMTZOYSOSDSUBSGMLOTYCZCTXANUCXZOADEOEJYBCLEULB LYXGMGORWYBNIGNRUWJATDKWTNSTJBVFQENEPZJCVWRRMXFFHEBPBGQZTDBCCMCQDYUYICLUZKGYRMAVIURGHOINFOGSJSSMACWITEPVYEMKEJ TPCQQMYWOBTBOCHUSNOE

C:\Users\user\AppData\Local\Temp\tmp3975.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701195573484743
Encrypted:	false
SSDEEP:	24:CXuIDWqLgX6vdVaxL46BNaYMbtbF+qEBHi7z/dd0Vc/6cUmeDs:ODHgX6vd0l4gnMbtbF+qEMPdNiTmcs
MD5:	2530C45A92F347020337052A8A7D7B00
SHA1:	7EB2D17587824A2ED8BA10D7C7B05E2180120498
SHA-256:	8BEAEA56B1D06BFFFE6142E95BC808FD28015E6A3FF32BC2FAC4C5A7552FC853
SHA-512:	78F4D4E93139D099D59F17867A6BB87A7DB92E1637A520B522A32DF14D18A39602F1C255C64C4C406BA45138294D9467850FEEA90C199D3434D60AE1C7F6B4DA
Malicious:	false
Preview:	DUUDTUBZFWQODSNPWYYAIDZFECIUBQYLVGHZRZFDGGWVZPGQSHTPZANMRMNDUZLXCVYYIRRTMYEOTHOFJLCKQKOCQKNMRKZTHKIIPBKXIKLDAZ FJGRVUHMDDXAMADOCGROYYDTNZZUEROBUVEGQEAZOMYVDGVHXUWCBVRBLFLWITRUFMXJJLQTZTWLOSFUMQDKRZDXVRLBYBKLXGLTGADROPECYT RYJQJWZDWJQHGRYFIQLJDBJUFPEPZLWGXGGDQGOLJCVZAPHJZOSIZQHISQFRJJGEZIJEFACYWHJRHAADQBMDQFJAGFBEZNQNGWDHSAAXOAEHIE HTAEPMOFJSOCRPTEUZGGSVYGVNUAYJPFNXFSYEEMDNDGDUBNXUOHVEJQBDRGSCASTDANAAFPQYQEHHTAOTYKYJJYXDZMUTBXBCIFNYSYWNMYAE EUEIGDANIBIJWTMCMGVDPOCAVEJZDTVMKOQPOOOKMLFWWMOASXZUZVHWZKPBVANJIBBDPCEKXDPEFNTXPTFJRBFUPHQCKMDMMXQPDZLJPURSOL PQREZLEFYXCGNKSFQRMLKDMGSNURCWGNTDQUIOYBPNJAYWOVTXRGROGVHNGIEDBYKUHNRBBDKYQXANPQWPKEOHDUBNRSQPALMLJE QFMXCQMEOAKBRREEJTYCHGUEGBGPJLGWRCLYLAKRESHJPMPCUHRFXHVUIQCQZYDTCNRGWVTYBMIILXIIIOGMHAQBLHFXCLTIKGXWDVRGSSRDNC YOVCLTUUEWRIDEOSWWZKTQLGLSIFPVAFJDGWVZYJUOVTMGGZMWUYOQYCLDNLMKWCJBKOXTWTPCMMIEYMISQTQCKMPNWJVAXPFISOGTRIMGKBHK EJOEDYIGOBOPVFADMXZUZQZVMUDYSPUHDXFZMAVPGIHURQNBZXXDWPSHUEZEFABRCKBUQLCPYBNGKJCWBTBSWMABCFIYQJOHFJJEPNNMRWWMNL OTWSMOXCILCCNICPDFTO

C:\Users\user\AppData\Local\Temp\tmp3976.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.692990330209164
Encrypted:	false
SSDEEP:	24:NCzz4hMQMxH70HULgnraTryj1S0KEX64u+O572j79DwzpnQf8A:axH70cauYS0k4u+O125wtnm8A
MD5:	DD71B9C0322AD45992E56A9BCE43FE82
SHA1:	60945B6BC3027451A2E1CFA29D263A994F50E91A
SHA-256:	19AC62FD471E562088365029F7B0672623511CF3E58F2EF6DE1A15C14A2E94E7
SHA-512:	86EA2B42FEB542977FCF534B4708F7A07E09F4ACC413307E660B905408BC4AA9E26C50E907FA02379EA3EBFD18C532CC9DC269B6EA5994E3290082E429CAAE0 3
Malicious:	false
Preview:	EOWRVPQCCSGUYRPSSKREBPXVQXUWKHGDIJHLBLYMXTIUESLNTSFMRJGDSQHOWECQAJMENKQNNWPVETUPWMXJTCUIAKPCZEENXVLTKYPKROZPDE BFNAJOVCNEXQJFUHQCMLNHGMRJJIPLOMWFWJKKXSTRHWFVLVQPEMFBLDTSCCSXADJIIDQIYCEGSDEDZDWUEJLTYJHMYEHHMBFZCRDHXZVPESWN DGUEFQZTJFSJVKZMWREMIZGAIZANQJKWWXITTXHDQDZOEOGKCEMDUUBDTMNWBRSOWEKQXQDCYJXERQRAMVQCWCTYJPEAJUAWNBRQ WGFJAHXJJFRYTZMSGCREPRECKHXXMJGSQEKUCUNCWUAAPBWQVSMWCJGYSLPHJJHJGXSMNLNICJMSGSWRKARHMQXLYSAOPDAPXSMO RZLUWYOQTJQNKSCAJWRUEYRFPNOVSMNYRKMTSGRIFLOAJUGJYDTLINOTCEADKRENVYNODFSIJGSDCICIDXZTLLSKKJQSOHYTZRBSHPHXWZOOSK QIRSGPTAOQPBVJAMXOGPYNJMJXAKCTMRRTFCBPOAMNJORWRNZOGZMNBVCCZYQPOQOUXBGKNLFSQWAWEREFQBRDLTVHEFNRUSOARH JPRECDRMPANZRBGCANIUWEBUDVWLYHFTPGBHSZBZBEFUWFHUZPJOVMHGSINZWDUKWPGMGSNSSJNOMETOCJILXRQRGZQFAJCWYQEENIZIMHRBTZ UYEOKCQXYLWCKFHOHCOVRVPNTEUARVJEFALBUVYXIYZRMGJWZNYNLPYHZSSCODVXZBIWXIOAVMGMPKCPYIFZIKWRIHNIYASXZLMOLNZOMMYUSC RZBCXRANWWODLPHCXXDPLNYLMHYIUYZJWQLECFNXQEERYDVDBPXOLGZLZQCVYUYKFZGKXWVDQANPXQYAATYFJALGENVLDMHDASWKNNXODUHLXY GCBUKEFWISCCUWXNUNETWMTQHQDJMAXNPFPLMPQO

C:\Users\user\AppData\Local\Temp\tmp3977.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6959554225029665
Encrypted:	false
SSDEEP:	24:TifvYKkubZMu3HGRW2lJUao1nH5o4WGAZ46:rKkmZMuklJUj+GAZ46
MD5:	DCABA2748DFEAEF0BFBC56FD9F79315C
SHA1:	B87FBA690A774893B22B9F611DFDCB5CDC520269

C:\Users\user\AppData\Local\Temp\tmp3977.tmp	
SHA-256:	86DF5957E0CD2EBDFC2FF8C2F05569BA71462149042DF57ECE5E8228E3BC5DDD
SHA-512:	65F10692D0AE5CBAADDB03E89D6CD1D3486429906437A17C2B1157BEDB069202B1DC52A4E864AA8F90B8CBD171FD2A3E150185BF7DFF81540E209B6A8F8829I 3
Malicious:	false
Preview:	ZGGKNSUKOPMPPNHVZHJQGVEFQIYKECDTBUUNZDYNGQNIRYRWHUTXXPSHQTZPTZVHQXNNQJMVUKUOXVGORIAYJGXFFBGSTKCIJZKEQXQQIVFFMJ LOMJSXIEOLRGDCSILZBJCYZNNVATINEQDJPDYKYEGAQWQMEKFVPOYVPNSSIUTCUVWRTSGVMOYKONZJJHVYYHDVZQPBVLAEYYFULQVIAJCQYCDC EGDPRRLXXZXFIPXZYSZYOHEAPCISCQQIAXVPAQUVHGATHPNBNNZVCLFBZBDBZXOQODZLPUONDHVUIQLSZFYHOZHZHEGULYTEVGGLQVDEJVLJEV PQFWMTICLCXTQWMOFFAXIMODRSEVRDYZWTZFYKVZAJEAQBNILURHKTJBNMYKYFSYGEEBYTRKZAHNYHNKUVIQXUDTDSCKKVFAHEOCHUYENGZNJL YIKKSHPNCIQVEDXXJBQWLPTRWDPYUIEDKEYQXNAFVHZZHVLORWXSFDRTMIHTRSJAHAAHMDOMCQGDKDFHBNGVZQTTCSWSPIHCTQXSLLYZTFMEMA CZONDWHGUSVOCWSBRSQZPAKSJHSWPMXYNSVNZCBVQSSDMAXHBCCABCBJMXUBBMSGLUNDNJSGZUMDVFIJNOELGIFULZKPJDVNZQPDOWCXYQGTVJ KDHOFHYVKNSZDNMILUISTCTZRFSEWRMDZLOBGFMXNVDCJYYLJUDJGSTSUEEGOSENKRNGXAGHHNOGGDSDRGIFROBPWJOCJPXDATRXEPUOWMBLLO QTSWYHGAJBORDMNUEAHWTKUYXIIPMYCMRMTPBVKTCXSHVYJOWCUSTTUMTZOYSOSDSUBSGMLOTYCZCTXANUCXZOADEOEJYBCLEULB LYXGMGORWYBNIGNRUWJATDKWTNSTJBVFQENEPZJCVWRRMXFFHEBPBGQZTDBCCMCQDYUYICLUZKGYRMAVIURGHOINFOGSJSSMACWITEPVYEMKEJ TPCQQMYWOBTBOCHUSNOE

C:\Users\user\AppData\Local\Temp\tmp47E0.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp47E1.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp7134.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp7134.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp7154.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp7155.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp7156.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp7157.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp7157.tmp	
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\tmp7158.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp7188.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp7189.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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

C:\Users\user\AppData\Local\Temp\tmp7189.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp9A21.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmp9A22.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmpC2D9.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmpC2DA.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\tmpC2DA.tmp	
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpF3DE.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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\tmpF3DF.tmp	
Process:	C:\Users\user\Desktop\Z5kAk5QCIB.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..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.513695191295041
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%

General

File name:	Z5kAk5QCIB.exe
File size:	369664
MD5:	6b372844c175aec62acc6cc18e1f8006
SHA1:	d2dba224689f9c3a2e5a3c1840a8d05e65208c29
SHA256:	8b0d5e431a0e9caab067ece82c2898714b34ee4da85058 6b4353ead178a1c67e
SHA512:	9f04475fa220020c0acd7321e45307eb5e8d73b7404711 9c5209c3d0bb3cc1cc0275fc9c5f951467d85dae6c1e48a 7b6e97cb25a82a4a486e35ec9cfcdba19f
SSDEEP:	6144:c2DsTSujX+adglCbYDl79eb37tbO6/ZNXqLm3Ngh reUSO1W:c2DsHjXslHD3IRbOeNX9CreOQ
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....".f.y.f.y. f.y.....M.y.....v.y.....y.o...e.y.f.x...y.....g.y.....g.y.....g.y.Ric hf.y.....PE..L...s..^.....

File Icon

Icon Hash:	aedaae9ec6a68aa4

Static PE Info

General

Entrypoint:	0x401c60
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5ED4FF73 [Mon Jun 1 13:15:31 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	9680696139920742654 63fec272c56c9

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1910b	0x19200	False	0.454990671642	data	6.23741926715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x8596	0x8600	False	0.284893889925	data	4.59156222026	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x24000	0x2768704	0x23600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x278d000	0x4770	0x4800	False	0.730577256944	data	6.47409657815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2792000	0x10974	0x10a00	False	0.0774788533835	data	0.999461911392	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:13:27.054362059 CEST	192.168.2.3	8.8.8.8	0xe3ec	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:13:27.090913057 CEST	192.168.2.3	8.8.8.8	0xfde2	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:13:27.076493025 CEST	8.8.8.8	192.168.2.3	0xe3ec	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:13:27.113656044 CEST	8.8.8.8	192.168.2.3	0xfde2	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Z5kAk5QCIB.exe PID: 4140 Parent PID: 1876

General

Start time:	10:12:57
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\Z5kAk5QCIB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Z5kAk5QCIB.exe'
Imagebase:	0x400000
File size:	369664 bytes
MD5 hash:	6B372844C175AEC62ACC6CC18E1F8006
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: 00000000.00000003.313769707.0000000002EAB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.391337431.0000000004AD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.393187019.0000000005D65000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.390510548.00000000048A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.391542368.0000000004B2C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 712 Parent PID: 4140

General

Start time:	10:12:58
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis