ID: 490259
Sample Name: RzDaHvcf7g.exe
Cookbook: default.jbs
Time: 10:15:49
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

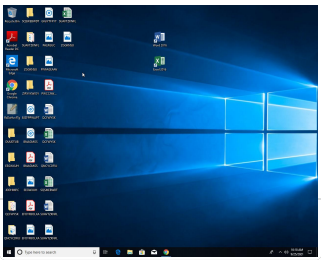
Windows Analysis Report RzDaHvcf7g.exe

Overview

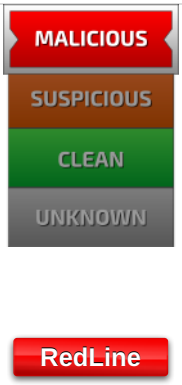
General Information

Sample Name:	RzDaHvcf7g.exe
Analysis ID:	490259
MD5:	fa4033de2f76c09..
SHA1:	3654d087b8d4d4..
SHA256:	f28cc6aa3c712a3..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

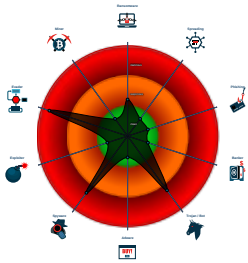


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- RzDaHvcf7g.exe (PID: 6344 cmdline: 'C:\Users\user\Desktop\RzDaHvcf7g.exe' MD5: FA4033DE2F76C09B47D1BCB6115BEA01)
  - conhost.exe (PID: 6384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.346746207.0000000003110000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.350203992.0000000005E15000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.347566779.0000000004BD0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.347119816.0000000004A6C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.254158682.0000000002F17000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.RzDaHvcf7g.exe.3110000.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.RzDaHvcf7g.exe.4aad876.5.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.RzDaHvcf7g.exe.4aad876.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.RzDaHvcf7g.exe.4aac98e.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.RzDaHvcf7g.exe.3110000.2.raw.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)

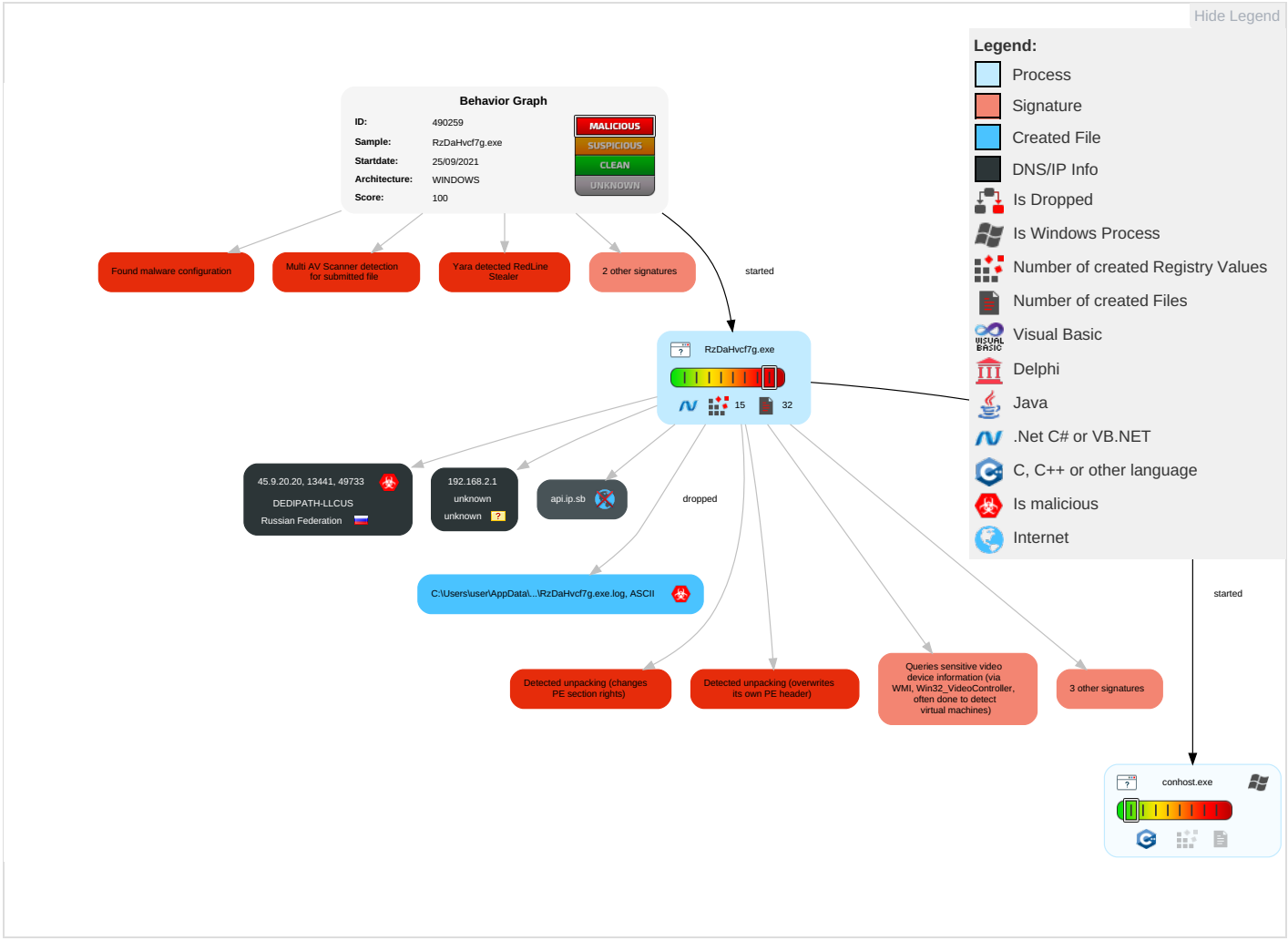
Tries to harvest and steal browser information (history, passwords, etc)

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	Netwo Effect
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	Input Capture 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	Input Capture 1	Security Software Discovery 2 6 1	Remote Desktop Protocol	Archive Collected Data 1	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 Local System 3	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
RzDaHvcf7g.exe	30%	Virustotal		Browse
RzDaHvcf7g.exe	54%	ReversingLabs	Win32.Trojan.Glupteba	
RzDaHvcf7g.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
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		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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490259
Start date:	25.09.2021
Start time:	10:15:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RzDaHvcf7g.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:	25

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@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.8% (good quality ratio 16%) • Quality average: 82.9% • Quality standard deviation: 26.7%
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
10:17:22	API Interceptor	66x Sleep call for process: RzDaHvcf7g.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.9.20.20	Z5kAk5QCIB.exe	Get hash	malicious	Browse	
	QH3hnrCD8x.exe	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	Z5kAk5QCIB.exe	Get hash	malicious	Browse	• 45.9.20.20
	QH3hnrCD8x.exe	Get hash	malicious	Browse	• 45.9.20.20
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RzDaHvcf7g.exe.log

Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKYHZHxLHG1qHqHs:Pqaq5qXAqLqdqUqzcGYqhQnoPtIxHbqU
MD5:	AC87262EF3296D7ECF33D548332613CF
SHA1:	4D9A75A7F7C75B4FF192D0D5B38E6DD735C85490
SHA-256:	C3A3112ED6BFC3837321F60C34BE7911E451185CA285F5B92376F417993B2014
SHA-512:	F38EE62232D98398B0704F5AB38718E9C97772F66FF188CC2072DD931FAEBFF3972D4E39511A01C8B42B7F43FE18917DCDEE28D4EE8FAAD6E6E256211101C90
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\tmp2F2B.tmp

Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp2F2B.tmp	
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\tmp2F2C.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp5071.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp5072.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp5072.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5073.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp50B2.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp50E2.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp50E3.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480

C:\Users\user\AppData\Local\Temp\tmp50E3.tmp	
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp71BB.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp91C7.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp91C8.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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

C:\Users\user\AppData\Local\Temp\tmp91C8.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp91C9.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp91CA.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmp91FA.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmpB1A8.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpB1A8.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\tmpB1A9.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmpB1AA.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmpB1AB.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.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\tmpB1AB.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD234.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD235.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEABA.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702247102869977
Encrypted:	false
SSDEEP:	24:GwASqxXUeo2spEcwb4NnVEBb2Ag1EY9TDqVEQXZvnIx+:nAD1U6+Lwb4dV42x1EIeVlXZ/5
MD5:	B734D7226D90E4FD8228EE89C7DD26DA
SHA1:	EDA7F371036A56A0DE687FF97B01F355C5060846
SHA-256:	ED3AE18072D12A2B031864F502B3DA672B4D4FA8743BEC8ADE114460F53C24D6
SHA-512:	D11ED908D0473A6BEA78D56D0E46FC05DAE642C6ED2F6D60F7859BB25C596CDAA79CC7883FEA5C175A2C04BD176943FF45670B19D6A55B3D5F29FAF40A19A 20
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpEABA.tmp	
Preview:	QCFWYSKMHARLAFTMDAYCDPDNVLLXYAHYJQVDDKWMWZXTODMVQHOWYAKZGPKJEHLDEADLWAOYFHCRBONQYOLNJKXLXXPSVNNBUMGS SHSRYIKKLNWBJSSZQFZBFWIPYYALBWYXPUCHCBPPPRVICZHAAXDBSBDAFSJSLRPZCKMILDLKTZJTTJWTRDUXPIOSWYRPJKVLJAGHSGEPPERRAQ LAJLIRGZPORRNBHIKYMYWHJJKNXIQOPDJPXFLFPWXDCSZYFDTACTIFVHTTSPLEYMJQGMJBZKBTPKCSRPHSAJZDKKKDYFDICXMYAQSFGBCKRXTF XXUYCXPOOHXIGGOZQXUOJXGUHUEOJLEOQQRFQRNQSWAOWAWOUVFMKBPTZVBCGRCYEHPXUWCDBHICKJYVGTNPPMEWNTSWYZNREIVB OXSICNBJXTOOMRYUPEHBVWMTIZHWLGFFTIUYFBQKZOWLOZMSGJFBUHXKMGISFGKCABOUUUQJAUODQPPYPQJGLZVADLCCGHPBEUWSDDXYCCQVTR QWCEJDTNAGHKGJTRWVAQBQJBUQWMJRXXASIQFFIUCPKMEXTJTVBDCBEYZDLKHCHQXMUBNRVRITBTYGULZYWAXVJAXNQEPONBFIAUWZCXQYHHPH ZWKKUTNXAQELCSUFKXKKQLLKNVNOREOWTEVCFHSUGPNRMAPAFPTHPGPAJPOCFBZXTIYQYUSEJFOUEZDUJSRXDHTOZAMMNCCIXWLXFQZALVARMP TDBNFJAJUMFQAHUJVWMEIDRIMZQXYHMCNBVLONHTHCXFAKSQBBXFBBFYSTIWNRKGOIHMIHZKIQSYCSFIRGLYFATERWSKAZLTFNMKHFVBLMXNER MNYZHBEYHNFPIPCGHZZMBNNYITUETKSXMZHNSGROLAGIITATFDCBZCBLYQHHYFPBDWGCTQNYPHDHFBNVEJJDIVMSPKDXKQBUNSMLJDVGOKQUEV KEVEUUSGEQJDKGYLPIDXNBIPBAJRUU

C:\Users\user\AppData\Local\Temp\tmpEABB.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6980379859154695
Encrypted:	false
SSDEEP:	24:A1cICRRGh4wXAyCbnhdKjiaeD+ICv1Ka42P:0cIYRGh4wXyny+VEV42P
MD5:	4E3F4BE1B97FA984F75F11D95B1C2602
SHA1:	C34EB2BF97AB4B0032A4BB92B9579B00514DC211
SHA-256:	59176791FFEBB86CD28FF283F163F0A44BEC33273968AADFF3852F383F07D1E1
SHA-512:	DD9C44C85AF10ED76900A2FE9289D28D99FB56CBE5385A46E485BE0F97A3EA7B119FE3235F334D84FA15902EA78F43C334424240B834D272849356421A33B207
Malicious:	false
Preview:	QNCYCDFIJJXXFOBBXUZWOFUQSSNNMFYIDILWLHTAZLHLJONMCDCVNCVXWBMUFJZAFKEEPNXZDYZJCSPOAMORBEETMACWAZGGTOXJCHTDTMVBHR PTLBCYZORACSZOXJZRVMZHVEOODGKJRRYLCKUFAYOXVKWJMPRNRNPZEPQZONIUXPPIZMRKSMXAPWYEFYYMMEVAXOVEZSPBEJXENHLIHXQMWJRN UJFILZBVCHZGSXSCZDLUJYAIEMFAKMGZRGVOACZDULPMTHUOBPJBMVYTDCJXFDPUECDSDSUEAFWGDFBMYZQEFBBNQHNIAZWLZMSUFKUWZABFJA THSHQHDIAVRZTRYPZQQLMBOTPFBQKJDTMNKBJAFYFAYVOMBSWHOBUQSYEBLHEDVKQNGPPYYDHQTDNFMKYJBWQRTHICJRWSTTREOOBMYGBUCHFD YMGHVLBDKHYWLYGTEDTHOSIOSXLWGESBKVKNDNLHUVLLUBIQJIAQTVGZHJBFRBPSLHGPZGCZVLETNOSXQRRSQJBXTKDASBHEZXYVHEIZXGANNJ HMIMQYHDFNNALGZYXGCPYFPYZSCSPKUMVVWIRDXSMSGEKGZNWWWVXGTXWDKSTXVLHRXFELLCWRSIFVJLOUVSMBXWSHSPQZUHHYPA NCFLOAYKMMBXMIXYFORAFUEVNVTQFWGSCJZEOHRNDHLLFYLQFOZXARKDDGYWBOFNOCUJWZALYSUEUOMQHCYTBHPYEDSSAKKDECQAZIWWHOJPIM NYUNNZPDBNECENBWFCTSDYUMRCXDFCNYFVTFUUWRGBGWUGZTYCTBQVNAVSKZCNNOJNXDSQUTVJLYJMHLQJJBPEDZOTOVFCJLUVQVIEYTFNEEDH KMXTEKAIHTQBGOPUGKWWNQTAGBHAUZVKMHWVZTYKYOWJYFEGCIPREWFGAHFXDMSFOAYRDJCTSGYNSDSELZDMIXRNFGOTYBEUKLAOAVMHJKZEBG SCQHGCDZCAAGIVBGWEQA

C:\Users\user\AppData\Local\Temp\tmpEABC.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69422273140364
Encrypted:	false
SSDEEP:	24:hdGRma8y0UOkmVb01yh9qfT+PsSMxto3vIcMhrzxYWSDHtj:hdGRma6bRh9rsFE/uhrOWSDHh
MD5:	A686C2E2230002C3810CB3638589BF01
SHA1:	4B764DD14070E52A2AC0458F401CDD5724E714FB
SHA-256:	38F526D338AC47F7C2CAB7AB654A375C87E51CC56B4FA09A7C5769E2FB472FFC
SHA-512:	1F2AA9D4B55B52C32EF0C88189256562B16DF13EEA0564BD7B47E45CC39279F39823033ADF95BBD9A50B4F35E417E418C4D20BBE14EF425EFF7134ECE05BEB3 F
Malicious:	false
Preview:	SUAVTZKNFLPDUIKIPSQJDVGAPGXKDOHYHNOWHLTUYHUBPZNAGHXWSRGELNTTLWSOVKHBKQEKGENMQDFUYQEFPUMFVGFHNHBEYAAJVHSIYLSLGV ZSSKYNEFOJGJXPWCGXOBRZVXDWDDKKLDGWVLNCMOJKBSBYFMTKILZOONEGLZWORUNOTXJNOTGXQTUBOXEFHVICNNYYHMRGCLTZLWQODATYJZBG FVEMSABDUIKNKVRGQOHHCSHZAJIYWZLGGZOOEOQBTEAFTXBQJIHRZBDRPFDGHVFGYZEIHFYVBPAXJYSLOTRVHEFEEWXUGJCOLFXEKSPFHBKQEH GPZADNNCAUYCTEDLFKZMZOQOADUCTDIOYKELVKGABHEMOSAYPWUUKTZHQNEQWLFATTPCULHLMBMEQVAXDFQNQLMLVOFTUTWLMJNL VNCRHTWUTJEEORGWISXALHDTNXRCWVMZRUEMSVOJYMENRHGVXXMGLOWYRFKZLPBZQMETPESMZPCJGYXVQSMCJXYEMMNKLPIXGOXO MQNYCFAEVPXDGOFEGSLWKBUOLRKXGTWDFUVGYFTOWQZAOIMQUZEELMCQWKUBEWGFDVXSXNGHPJNVDQHMPSSIFZTQLVBBHZOEGNPD AWAYLIRBWZHXRAXBBESYNRIRINAKLQMELNYRHRPKDBUCNSZOVHNTBCUYDQTGFWZJUCUZBHHXHQHKWOWTEWLUGGGWHIHCWZLLJPDFVDICZBBLFS ECTLMQBKCPCHANOICKIUSVAJTYQOIUWRGVAFOFTMIHARUUCNGBLVFIKMTTGPYXNEVGLPMZDMIQDQOLIEFHNZYMZTCDOHBNQLNVLXRUXMGYCVOJ DBWPSJKMFMEDBEMXULQBRVRKPYNUACCXNPGFEMPXDXNEIPTKGSKUMVFSLCTJFHNFATCDKSZWKYMVQNTVHCOAJXDUTJZESFLKTQOGREXBTBVBGL DYJYDTNEAQDFRTXMJIHJCCTPUDZLNKNEABFQYCDL

C:\Users\user\AppData\Local\Temp\tmpEABD.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6969712158039245
Encrypted:	false
SSDEEP:	24:zDLHcjI8IQ6sNUYzo1jfRRMF6zzC3ZzNTWx7M00:zDL4ImUYzebRR66C3Z0JMR
MD5:	31CD00400A977C512B9F1AF51F2A5F90
SHA1:	3A6B9ED88BD73091D5685A51CB4C8870315C4A81

C:\Users\user\AppData\Local\Temp\tmpEABD.tmp	
SHA-256:	E01ADE9C56AF2361A5ADC05ADE2F5727DF1B80311A0FDC6F15B2E0FFFACC9067
SHA-512:	0521ED245FA8F46DE9502CD53F5A50B01B4E83983CC6D9DE0CF02E54D2825C1C26A748CC27E24633DA1171CE0309323235ECF7EB536D4058214D7618794CF2F
Malicious:	false
Preview:	PWCCAWLGRESZQJYMKOMIHTZVFVPFCSAZVTKGMPWIGSDMTLFZQLHJERDPYZCJGFCRLISWNBAMIMDXCWDVGVLWLRBEVYOOPHYWACKPZXSURGSIFW TFUJKLSAQNAJEWDLUIKFHXLUAMUDGRAVFMICAHEZBIIEGWGAVVJHMHSIBGNLEHYVSOKQMYABDYCPEBOGBMYUCIGVRGYYQRAYNYHAIBMHOTRIZL LYBECMXTCFUOVXXHSEMIUWSBDHOZIZZUXFTLKXXNEMXBKLCQDPKVZNOMDYUYJRWCVILZVJDNNBMPTNOFSKRQTILJRXTKDNUIYSQCAOPCQKTXYX PPGZDZOQYLGYFPFIWNBSQZXYABPTNBJQNBZEETJSFXZNHXBRWUHOMCZAGZQJLNPMZFALBBPHBIXZHLBTBJLTUHPUYVUDWDFJANSIIDJVMUYLPZ PYGAJWMTOHGILQWHKJDQUWMTSWIBVVZGAHCNWIFZNGNERRKMSIVXWXEXRZZEWYASCIYJYCOOBWRTNZELPWKFVZKZIBGQBLGCTSTNAJSWPHYJCQ SYZVFRYFSRAVVXJIOHQCNVEOIMWPEAVCJLBHRUKDHJWPFMXAKTZVQCOUKYCBZFWBREKKHOHZVNMMJZGWIZEYRAIKTHMJRCWVWKNMJNSZHSDRUZ SQOJKCTOSNGKOKEAWUIQNIYHWKIIDHKQIJWCSGRRLEVUTENXSNNVDVYDJTIWYNCAZIEBXMIROLIBTLMGEUOCECFFWLENTJSVHFKQHKAPBXQAJJ SUOUSFCBQTHCFYZGSVVAUPLQELRWLXRCZSUSFUBCORCWMJPUNHTEEYODSFGJFTDZLLXMQYMIHIZXOYGABIAWYSBWLAJSCKBWGJBVMMJKBKLUHU LJIUHQXIXESAUTNVVZNKMIVIOHPPQAWTQSEHTQMIWNPRZRETXZHRGWOTGIEHCCSGIUCKCIFCQPTAJOFCIMYSMCOPGASEEYCNQLXCNRAPQUSQXT WPKPYCQXPE

C:\Users\user\AppData\Local\Temp\tmpEABE.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6980379859154695
Encrypted:	false
SSDEEP:	24:A1cICRRGh4wXAyCbnhdKjiaeD+ICv1Ka42P:0cIYRGh4wXyny+VEV42P
MD5:	4E3F4BE1B97FA984F75F11D95B1C2602
SHA1:	C34EB2BF97AB4B0032A4BB92B9579B00514DC211
SHA-256:	59176791FFEBB86CD28FF283F163F0A44BEC33273968AADFF3852F383F07D1E1
SHA-512:	DD9C44C85AF10ED76900A2FE9289D28D99FB56CBE5385A46E485BE0F97A3EA7B119FE3235F334D84FA15902EA78F43C334424240B834D272849356421A33B207
Malicious:	false
Preview:	QNCYCDFIJJXXFOBBXUZWOFUQSSNNMFYIDILWLHTAZLHLJONMCDCVNCVXWBMUFJZAFKEEPNXZDYZJCSPOAMORBEETMACWAZGGTOXJCHTDTMVBHR PTLBCYZORACSZOXJZRVMZHVEOODGKJRRYLCKUFAYOXVKWJMPRNRNPZEPQZONIUXPPIZMRKSMXAPWYEFYYMMEVAXOVEZSPBEJXENHLIHXQMWJRN UJFILZBVCHZGSXSCZDLUJYAIEMFAKMGZRGVOACZDULPMTHUOBPJBMVYTDCJXFDPUECDSDSUEAFWGDFBMYZQEFBBNQHNIAZWLZMSUFKUWZABFJA THSHQHDIAVRZTRYPZQQLMBOTPFBQKJDTMNKBJAFYFAYVOMBSWHOBUQSYEBLHEDVKQNGPPYYDHQTDNFMKYJBWQRTHICJRWSTTREOOBMYGBUCHFD YMGHVLBDKHYWLYGTEDTHOSIOSXLWGESBKVKNDNLHUVLLUBIQJIAQTVGZHJBFRBPSLHGPZGCZVLETNOSXQRRSQJBXTKDASBHEZXYVHEIZXGANNJ HMIMQYHDFNNALGZYXGCPYFPYZSCSPKUMVVWIRDXSMSGEKGZNWWWVXGTXWDKSTXVLHRXFELLCWRSIFVJLOUVSMBXWSHSPQZUHHYPA NCFLOAYKMMBXMIXYFORAFUEVNVTQFWGSCJZEOHRNDHLLFYLQFOZXARKDDGYWBOFNOCUJWZALYSUEUOMQHCYTBHPYEDSSAKKDECQAZIWWHOJPIM NYUNNZPDBNECENBWFCTSDYUMRCXDFCNYFVTFUUWRGBGWUGZTYCTBQVNAVSKZCNNOJNXDSQUTVJLYJMHLQJJBPEDZOTOVFCJLUVQVIEYTFNEEDH KMXTEKAIHTQBGOPUGKWWNQTAGBHAUZVKMHWVZTYKYOWJYFEGCIPREWFGAHFXDMSFOAYRDJCTSGYNSDSELZDMIXRNFGOTYBEUKLAOAVMHJKZEBG SCQHGCDZCAAGIVBGWEQA

C:\Users\user\AppData\Local\Temp\tmpEABF.tmp	
Process:	C:\Users\user\Desktop\RzDaHvcf7g.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69422273140364
Encrypted:	false
SSDEEP:	24:hdGRma8y0UOkmVb01yh9qfT+PsSMxto3vIcMhrzxYWSDHtj:hdGRma6bRh9rsFE/uhrOWSDHh
MD5:	A686C2E2230002C3810CB3638589BF01
SHA1:	4B764DD14070E52A2AC0458F401CDD5724E714FB
SHA-256:	38F526D338AC47F7C2CAB7AB654A375C87E51CC56B4FA09A7C5769E2FB472FFC
SHA-512:	1F2AA9D4B55B52C32EF0C88189256562B16DF13EEA0564BD7B47E45CC39279F39823033ADF95BBD9A50B4F35E417E418C4D20BBE14EF425EFF7134ECE05BEB3F
Malicious:	false
Preview:	SUAVTZKNFLPDUIKIPSQJDVGAPGXKDOHYHNOWHLTUYHUBPZNAGHXWSRGELNTTLWSOVKHBKQEKGENMQDFUYQEFPUMFVGFHNHBEYAAJVHSIYLSLGV ZSSKYNEFOJGJXPWCGXOBRZVXDWDDKKLDGWVLNCMOJKBSBYFMTKILZOONEGLZWORUNOTXJNOTGXQTUBOXEFHVICNNYYHMRGCLTZLWQODATYJZBG FVEMSABDUIKNKVRGQOHHCSHZAJIYWZLGGZOOEOQBTEAFTXBQJIHRZBDRPFDGHVFGYZEIHFYVBPAXJYSLOTRVHEFEEWXUGJCOLFXEKSPFHBKQEH GPZADNNCAUYCTEDLFKZMZOQOADUCTDIOYKELVKGABHEMOSAYPWUUKTZHQNEQWLFATTPCULHLMBMEQVAXDFQNQLMLVOFTUTWLMJNL VNCRHTWUTJEEORGWISXALHDTNXRCWVMZRUEMSVOJYMENRHGVXXMGLOWYRFKZLPBZQMETPESMZPCJGYXVQSMCJXYEMMNKLPIXGOXO MQNYCFAEVPXDGOFEGSLWKBUOLRKXGTWDFUVGYFTOWQZAOIMQUZEELMCQWKUBEWGFDVXSXNGHPJNVDQHMPSSIFZTQLVBBHZOEGNPD AWAYLIRBWZHXRAXBBESYNRIRINAKLQMELNYRHRPKDBUCNSZOVHNTBCUYDQTGFWZJUCUZBHHXHQHKWOWTEWLUGGGWHIHCWZLLJPDFVDICZBBLFS ECTLMQBKCPCHANOICKIUSVAJTYQOIUWRGVAFOFTMIHARUUCNGBLVFIKMTTGPYXNEVGLPMZDMIQDQOLIEFHNZYMZTCDOHBNQLNVLXRUXMGYCVOJ DBWPSJKMFMEDBEMXULQBRVRKPYNUACCXNPGFEMPXDXNEIPTKGSKUMVFSLCTJFHNFATCDKSZWKYMVQNTVHCOAJXDUTJZESFLKTQOGREXBTBVBGL DYJYDTNEAQDFRTXMJIHJCCTPUDZLNKNEABFQYCDL

Static File Info

General

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.515668919401783
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:	RzDaHvcf7g.exe
File size:	369664
MD5:	fa4033de2f76c09b47d1bcb6115bea01
SHA1:	3654d087b8d4d4e3d159234f5633c96592539943
SHA256:	f28cc6aa3c712a3e9d8876e15d385c8854d1a1a65897f84edd794ed1f47af2e8
SHA512:	e4d0bd9d5f885eabda3b2f7932b909efeaaeaa5eda5b35afd84113189d9e9a248cb67f8fead78d7d923e8d2bdb5c83103532ca76d52beb2be92c831f4144d971
SSDEEP:	6144:S2bMzpbjXulCbyDvvtMf4w+FlbU2zHFnBgK4feO+z4hQzp8U//F:S2bMtjXultDmfubUIdB+fe1znp8U//F
File Content Preview:	MZ.....@.....!..L.!This 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.Richf.y.....PE..L....._.....

File Icon

Icon Hash:	aedaae9ee6a68aa4

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, NX_COMPAT
Time Stamp:	0x5FE9F0FE [Mon Dec 28 14:51:42 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	0.454912935323	data	6.23817145476	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x8596	0x8600	False	0.28562266791	data	4.59688759532	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x24000	0x2768724	0x23600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x278d000	0x4770	0x4800	False	0.730305989583	data	6.48345648688	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 10:17:21.083441973 CEST	192.168.2.7	8.8.8.8	0xb6bd	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:17:21.121860981 CEST	192.168.2.7	8.8.8.8	0x18bc	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 10:17:21.104016066 CEST	8.8.8.8	192.168.2.7	0xb6bd	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:17:21.148773909 CEST	8.8.8.8	192.168.2.7	0x18bc	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: RzDaHvcf7g.exe PID: 6344 Parent PID: 2148

General

Start time:	10:16:47
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\RzDaHvcf7g.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RzDaHvcf7g.exe'
Imagebase:	0x400000
File size:	369664 bytes
MD5 hash:	FA4033DE2F76C09B47D1BCB6115BEA01
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: 00000000.00000002.346746207.0000000003110000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.350203992.0000000005E15000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.347566779.0000000004BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.347119816.0000000004A6C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.254158682.0000000002F17000.00000004.00000001.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: 6384 Parent PID: 6344

General

Start time:	10:16:48
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff774ee0000
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