ID: 490248
Sample Name: aVfFzvm8iR.exe
Cookbook: default.jbs
Time: 10:05:10
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

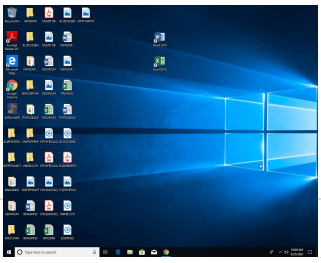
Windows Analysis Report aVfFzvm8iR.exe

Overview

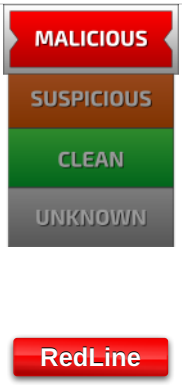
General Information

Sample Name:	aVfFzvm8iR.exe
Analysis ID:	490248
MD5:	6991603097a011..
SHA1:	c7d00bf33525837.
SHA256:	111d1312a6f53b6.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

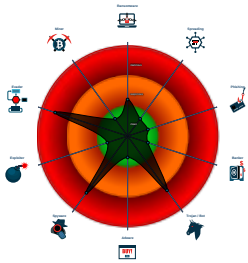


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Detected unpacking (overwrites its o…
- 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
- Queries the volume information (nam…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- aVfFzvm8iR.exe (PID: 2904 cmdline: 'C:\Users\user\Desktop\aVfFzvm8iR.exe' MD5: 6991603097A011D73B25213DBA357B93)
  - conhost.exe (PID: 5228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.358831451.000000000211C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000003.272708961.00000000005CE000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.361464127.0000000003645000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.359419486.0000000002320000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.359783464.0000000002540000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.aVfFzvm8iR.exe.2320000.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.aVfFzvm8iR.exe.215c98e.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.aVfFzvm8iR.exe.2320ee8.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.aVfFzvm8iR.exe.215c98e.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.3.aVfFzvm8iR.exe.5ce160.1.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

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

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)

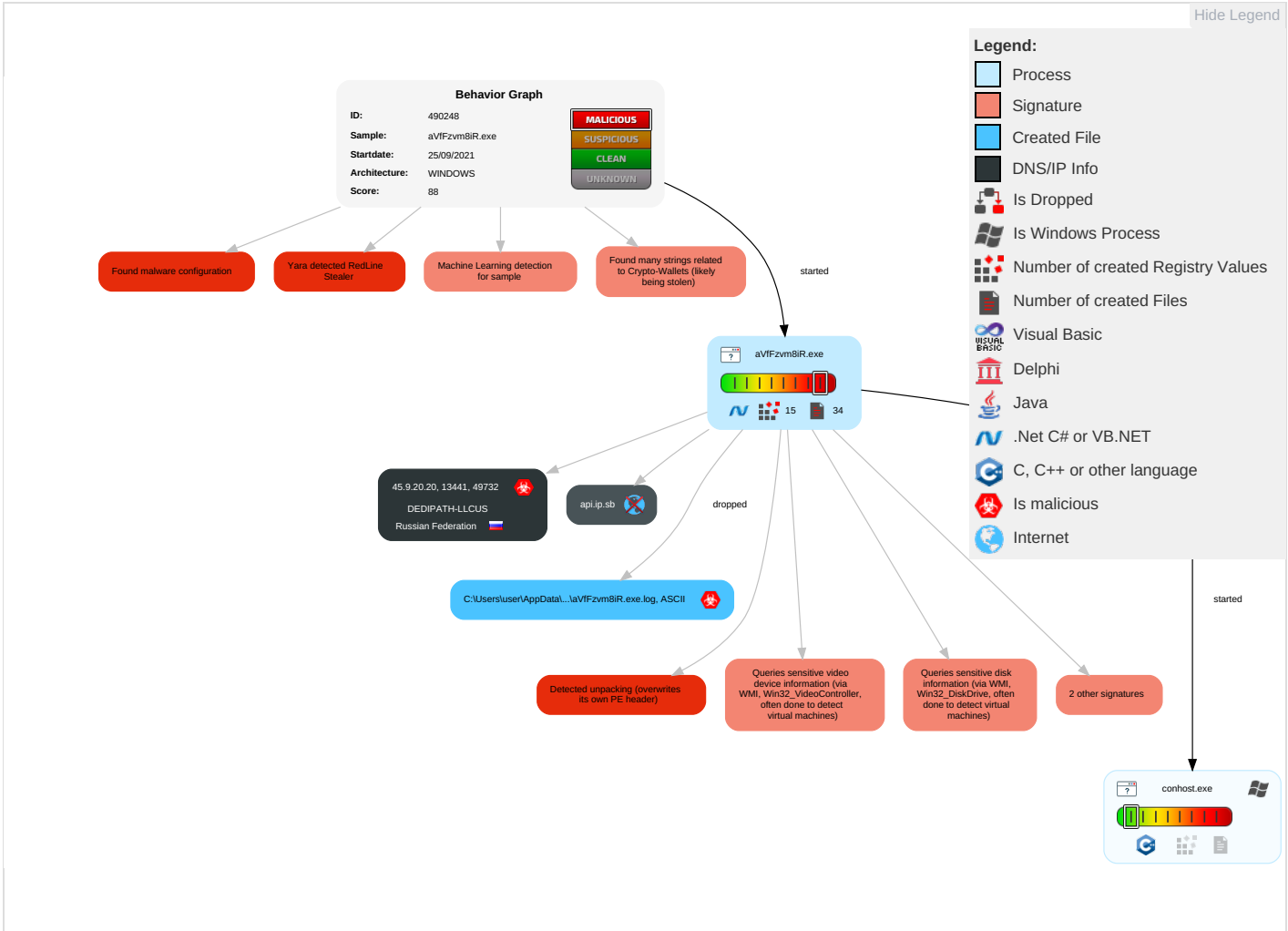
Remote Access Functionality:

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	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 3	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 1 2	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

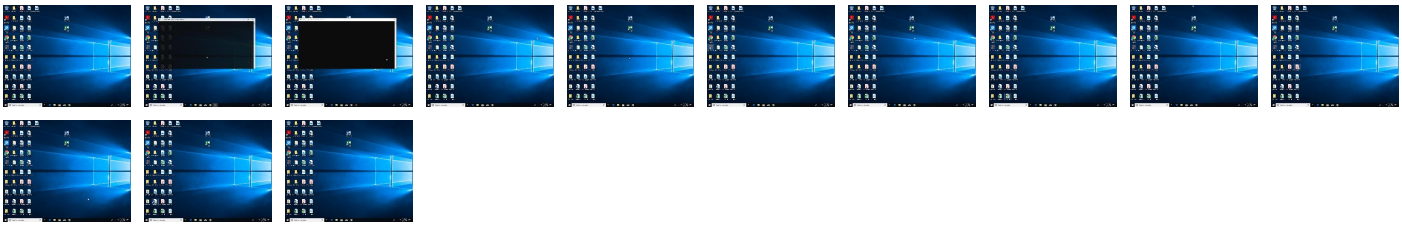
Behavior Graph



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
aVfFzvm8iR.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.1.aVfFzvm8iR.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

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	
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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490248
Start date:	25.09.2021
Start time:	10:05:10
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aVfFzvm8iR.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@2/29@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13% (good quality ratio 12.6%) • Quality average: 84.9% • Quality standard deviation: 24.1%
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
10:06:53	API Interceptor	67x Sleep call for process: aVfFzvm8iR.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.9.20.20	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	
	6C1rDzuqhW.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vrZJf2r6Mz.exe	Get hash	malicious	Browse	
	4gbNkZQv4g.exe	Get hash	malicious	Browse	
	N1T31rqZU0.exe	Get hash	malicious	Browse	
	y1ULNwRnc7.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	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
	6QnP1PXwHi.exe	Get hash	malicious	Browse	• 45.9.20.20
	DUIuBOErSU.exe	Get hash	malicious	Browse	• 45.9.20.20
	3F6611DE6461742498699116526CC1EA93CB24C010B24.exe	Get hash	malicious	Browse	• 45.133.1.179
	Quotation Sheet,pdf.exe	Get hash	malicious	Browse	• 45.133.1.47
	dVJXoBazmx.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\aVfFzvm8iR.exe.log

Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKYHZHAHxLHG1qHu:Pqaq5qXAqLqdqUqzcGYqhQnoPtlxHbqS
MD5:	66D7E07C835F707963009A207CDC770B
SHA1:	8D3D65EA8FD18976FF325E0812F0DD8B6C12F275
SHA-256:	7840FE961948856C25B191A6013E8694CC8E0B80F7B8A6A474C45EB0FB53A336
SHA-512:	F36B511EA43599DB92751D8873EE429D8B5D342BA14E8C9EEC9250A21C2373B2EF10E4E6C8372B8011023FAE8B76E04CF09557186CB6D5B28C44408F661C7955
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\aVfFzvm8iR.exe.log	
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\tmp2303.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2304.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2343.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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:	high, very likely benign file

C:\Users\user\AppData\Local\Temp\tmp2343.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2344.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp2345.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp2346.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp4AC4.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp4AC4.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\tmp4AC5.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp4AC6.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp4AE7.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp4AE7.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5C07.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701704028955216
Encrypted:	false
SSDEEP:	24:t3GWl91lGAaII86LPpWzUkxooDp2Eb6PEA7lhhzhahpmvYMp+wq2MseSnIrzv:t2Wl91lGAad/xoo12e6MyF4/jMp+t2Mh
MD5:	5F97B24D9F05FA0379F5E540DA8A05B0
SHA1:	D4E1A893EFD370529484B46EE2F40595842C849E
SHA-256:	58C103C227966EC93D19AB5D797E1F16E33DCF2DE83FA9E63E930C399E2AD396
SHA-512:	A175FDFC82D79343CD764C69CD6BA6B2305424223768EAB081AD7741AA177D44A4E6927190AD156D5641AAE143D755164B07CB0BBC9AA856C4772376112B4B2
Malicious:	false
Preview:	BNAGMGSPLOQNKLVQWYYWYGDTNIHHPSGKYBNBNGFSZGYYFUVNSOYTAMZPOIOKMFFWDJIYCJGTWZSMXADBSJDEKDTPXDVYBIZFLSTFISYXAKAYQW PLDFAWXXNTSVHRLCINNTRJHMBFQAQBHFRSHDDRJZGIFSOFSRODXCWFIUZRXRQSOCPSXKXNEHLQYKIBJRTMMHJOIZSWESTHTXPULAPGLZHBOLMP QWYSWWOGRJQGYWDWWZMHZMTDMRWBSPIXHCFFOHTJSOAULKIFZVXPTYEBTBEXGQNBQAECQOJGHTKIAXUJLSLPBKTTRORROLNTKPDPOMSZBBLUYF RZXYZSVBGBEMGTACDCBJNXKAMZMCYEWGKSUENLKBJSZIPKQGYXMJTJXBELNVMAZHRUESZSTWROIUXLLMQPYLVQYLCOMOCGPSMJQGILSDDRUUXD RUCCVECNPLWHJLTHCPBZIKDUNRJMJIOQOCHVVNIQFFXFKFHTCVEEAXHTLJMWIUAWAMHGIGQCQJZGXBEDCRRZCNVYKCPWVJCRXIGXZYJENNARSZ ZREAOODIGZVBXFPAHTZNKNQHLNNETJICOVQGFLQSGSLCOYMPYDSGOPNUXAMCIJBJPJBAABYHKBKWCUAXUHNOCSSTHZYJXPLMFVJQAJDDSNEVXL RUYEQEKUKUIAOQAQJMNLHOUFLFUDMCWRNYNNLOACVSDXDNNBOGQOYGOZTWUOFZYLZQXJEGPQNQFLLILMQUJLCLUOOAOAQRCWMGKH GFJRPSFVQPCSCUDFVYSGDQIHJWSUDEAMVIANGMMFSJJTPNRYYSJYDFLUXJZGSYAAUHOEPMQIZZRSZDCXHRCIPUERSVKWEBDJCXEWWKPAHBVZES VEWPJTYRBKLHQRRPGDGQPGTNNFRMWNTGWIZDBPSGFQDFZWTVLRAOKRBHWFHBPZUBSCFBAMHEWXUIUXMKHPOCNYWNKSRYBQKSUWJL JRNBFNMTDBSZDXVFSLPDQEDCNYELVD

C:\Users\user\AppData\Local\Temp\tmp5C08.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690299109915258
Encrypted:	false
SSDEEP:	24:0C2jKPS/GeHBPaNDdBKW/PXAx+sTTqBVw8tk7LI/csnfv:UWKPaNjKW/PwxfTixkY/cSfv
MD5:	F0D9DE697149ECBC1D88C7EA4841E5BD
SHA1:	06A2A47C12B3554397AA0C8F483411CAB366947D
SHA-256:	5BE0708B77E41FC490ECEC9CDFF20C9479FC857E47CC276D6F68C0895EA68FB2
SHA-512:	E9953E00241C3FB48E267F1A49E2C53FEE4240415C7A48FAD089742C6C4AA1C5A9CCFEE616FC91EB29C1C8252A3095163A515ABA96A1F0B41A8B12992969691
Malicious:	false
Preview:	EEGWXUHVUGUAGDCAESAKQJADEXSKGQOTKSMYVIQMWCXKMREFNGUJHWRPPFJWEQHLMDSTAHLHBQSXLRGVYEPBLZILRXLTPZSELULGEDFWQHJHNI HNCTGEIAAPQHNOFANJGPRIYVQSOFCGDPFBTNYILXIPYTWVOYXFUCEEQWZRPXFERZCPKKZAHOYWHFAYDMSXERUPTEZISMPADRFDIWGTWAXETEOP JYWDNGCDFFZUXZZSPZVIILCQXOFDOGUOSZYPXXVLSNAWWPHQGNSYQXOUOGPFDMDNPFUONUSGUOUKYHHGHFFZYEDSZVDRUEJKGSHEMJARIAEZZD BZJFCMNUJIHQFHGDONGFEZRYCZYIAOXAXGWENMTPOKNMZPJSZVCDZRZPFIIYHXITKZBLAJXANTSBCWIGABZKBTKDJRSTSKYORPMNGHCZWCLOVF PZBMYKBYDRXMFUQJDNWZFCVEOXPGJMBQZRUEOTLHEFHKDZLVFBXLUSXRAXKVLWGOWARAQZHIMTYBWKPLWNJFMLQVXGRMIGEIPZEIFBYZRYNEEZ HFMFOGMBEWLJPBXWVYHVEUKSKVKINVMDJKCSAOUXTMIHLOJXLTEKLKJDYABXRPKNGFOXISIFXHABTYQIPUCFNIJWNCTAFGYEIBCCNXPZQAGPHN NRICKSKCXWERLWTFSJWUSCBTVWSYUVWXJQHMSZYHAHYELYFPIBFZETDRPQBQHKMCXRRCAEYFIERXQZVCDZZBPQJJDQUDHKPMDBXPEBPFURYAPU WVWVJRWXHFXQGMVUGOILYXGFSMEFMKLBFACOSIKHHXRBRGYVIVAOTFNIIOQUZTHBZGOGPVUVYSYNHRKOADWYTLCNTHHCZYXXGFCXMFHZBZBCCM TYSROXNAHKABYAXPWRNKHCJYLAMQAUZBVJWHFXISFSKFXGFPDIOTITGPUETUYHRIXQOTIGEVDQWEBJVPDIUZVQFUBWREJIPSNXDGEKXKULZFHZ QHQXPMBIYA

C:\Users\user\AppData\Local\Temp\tmp72D2.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp72D2.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp72D3.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmp7B49.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6998645060098685
Encrypted:	false
SSDEEP:	24:FzrJLVfPTlXwAGfwXz0vRDC0aYECjYTixDXXwDyDFdJCSuHFF03T:FRLVHTlXwAGEoVCRYF0EDXgDVFHUj
MD5:	1676F91570425F6566A5746BC8E8427E
SHA1:	0F922133E2BEF0B48C623BEFA0C77361F6FA3900
SHA-256:	534233540B43C2A72D09DBF93858ECD7B5F48376B69182EDBCA9983409F21C87
SHA-512:	07D3CA8902964865FE9909054CF90DA1852678FBE58B1C0A8C2DBA2359A16DCBD43F23142D957DB9C1A8C2A1811EF4FEA74B0016A6F469538366B4FF01C8A14
Malicious:	false
Preview:	NVWZAPQSQLDLCZFLTMOWSKLFWOMMGYWWTZSPFFTDRHOTSSRKDGSJCIGMJJNKHMSAEMKBPGYCFVANNLUHHUMQOHINWJABNFIWWWZX JLCANQSKWMIWKPMVTCWFUMQBAGWZRWHRCMJDSNPGGGNECNQGPIZXLBIMLXMHDDXDKVYPEKRCNITDGJJNAEAATOVDDPBUDYWRPDYW ARJTFXBUUZABBVURIWKONIVMPCYVUBTOTCIJJVRWYUNYHAFJZUMVTOIXZGAVVNSRENTVPHFLSLFWBLPFQDMQCJIHRXSQOTPSPDZKXCRBHZXDQI ECBJTNIRGCACNADPHRWIVAWGPANEMHGPPPARWYWAOAHPWQLEGOBGVNWVBIFLAEOZYELRFOEZQCQIXCQBUKZGPOQFLHFLCFTYWBDGCWMDWICTIC WVZEAQNJOOVCGQZYTBBXQPEYFQMSMETMKKZMRGXXLCDXDEEEJKZAUNEWZONYMVVIZOWQRUQYNOEFMWEVWXFAZRHGHUXGAYODAXDN QONZPVBKRYIOLZJIYSHJSCEPYVMYISKJIWPKVGUQBNLZCUFGXBFZDDRGUMCLJGJPDAZKZLRMDSBFEJQYNNKTHBMJMUHVUOIVZRULJFFYIUMOHU GCJUYZGXKXNIWZUKRIYDZATEOXGMHUPOOBIHEEVPKQEZDDWJHKEKLNTMWMDCFDOYCCDOERYFZNFUDEHYXIBQAVVOHQNIEWZODOFZDFJSWYCJMW WOIZSCZSZBGOIFHRDBXHKMCCLSYNVVXYLWKXEKVHIZEBIBHWMXDXEGZDYWRROMYHTDQVCLXOGVHWHFNIDZOXWTTPAMAKJIYLNQIEDSCCTSBLPH TTGLCIYXXWIBXAGYBACOKOTPPBKACWQBYRTKFMCSSRYQNESLPTLSLCWCSLHOGHNCGUFWMYXDBUFSOKFIDUIBHTQJFIQTVZZVIZEWTBSHJWKQXG UWLFKNDUSKPDSMJNJJNEEOWEHOKTNZWRDNOXWJEK

C:\Users\user\AppData\Local\Temp\tmp7B4A.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.685942106278079
Encrypted:	false
SSDEEP:	24:e80g32tqxncx15PRgoZOZUxcz6oV0dh0dxiXMK:e87SH5Go0ZeuDufAiXMK
MD5:	3F6896A097F6B0AE6A2BF3826C813DFC
SHA1:	951214AB37DEA766005DD981B0B3D61F936B035B
SHA-256:	E6E3A92151EEE0FCDF549A607AE9E421E9BB081D7B060015A60865E69A2A3D60
SHA-512:	C7BD241F0E71DC29320CC051F649532FFF471B5E617B648CC495413587C06C236AFA4673A7BC77409E989260278CDEF49BDACA38BEB6AF65FEE74C563775B97
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp7B4A.tmp	
Preview:	PIVFAGEAAVVMYOKLIHAGVKQSIBRMIEBPKZHRSRYSYCTZASSEWGQLTFYPITGFBLIMOSZPCOYJLDMIKUYRMFZNOVAKNNFUFMFWAQZIZZSOHPUKTM EQKVMZGORRHHUAPAVEHNTRHFTCOWUQLMTXHFAASXNSJOMVEVZKIBTYUEOEAYWORCLXNWXMWVTCVFUJOOHJFVBTQGYSPLVNZVQAKY RWBXASIFOBPMFAPMAVEFPAYEVCHLKOVGMAFTDZYSFCRVFLUCDEZSALOPZIFCHRCOADKGTQMGRAQFQVFLPTIZCOVQGXVCITLOKGAEHQOUDVVLBL ANQIWAMALJXSPVCLVLGENZFIFSPDTQOOAOXTRKMORBXQQUMCVCGJNJNIYGXUUXANSJRSROPOUDFHQHUUMMRXDQWLRABBQAZENYVIBHRRHTGWSI VVUQDLCOQYLVPAUFYYHGIERJJLVMIHLHHCCGHRLMANSNVNAYHLENOWUETBHLULUXLDUIUWHDTSBTXYABZUPEVNUTYDIYOWXZQQWZTIKHRACSWY ILZGJJAYPXSWVAJEAMWRWUWIOONUGSOWTNWVILBTRYWXPSGGJYETTQICCTQMOORSZENPULBEQOBSNDWJHFGZOXAYRMRTCQAGZFKLTXQJCKKKJT XRIIVBYSWRFFSDWLAWEVZNFVJIYAKGOFIKGKPALYKLUSFUZNXBTTGJQARLJLEPNMUPZBHUFERZBUARRWLRQMAELUFJHXEPWKNEOUOFWRPCGUFY JEWTUPSXMLBAGQWILTIUMBXONDPOFUHNKJJKISPTLDQHMYGKSUZUEBYHKNHJUVSBOBSFQWTBGVEFNVAAKMXTORQQDIBVTWEQECBUJMCLMNPNRT KIKGQQLCBXEDYYHZALQNWVUKKTUNZMKPSISXIDNZZXVGUERMWOJYWVPNSTVVUORBONVDVVOSICVUMWTQLGBVUNLJTMTSZIJARQMRHCGASSVBBF IRIMTSICIANQBRVHJQBP

C:\Users\user\AppData\Local\Temp\tmp7B4B.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701704028955216
Encrypted:	false
SSDEEP:	24:t3GWl91lGAaIl86LPpWzUkxooDp2Eb6PEA7lhhzhahpmvYMp+wq2MseSnIrzv:t2Wl91lGAad/xoo12e6MyF4/jMp+t2Mh
MD5:	5F97B24D9F05FA0379F5E540DA8A05B0
SHA1:	D4E1A893EFD370529484B46EE2F40595842C849E
SHA-256:	58C103C227966EC93D19AB5D797E1F16E33DCF2DE83FA9E63E930C399E2AD396
SHA-512:	A175FDFC82D79343CD764C69CD6BA6B2305424223768EAB081AD7741AA177D44A4E6927190AD156D5641AAE143D755164B07CB0BBC9AA856C4772376112B4B2
Malicious:	false
Preview:	BNAGMGSPLOQNKLVQWYYWYGDTNIHHPSGKYBNBNGFSZGYYFUVNSOYTAMZPOIOKMFFWDJIYCJGTWZSMXADBSJDEKDTPXDVYBIZFLSTFISYXAKAYQW PLDFAWXXNTSVHRLCINNTRJHMBFQAQBHFRSHDDRJZGIFSOFSRODXCWFIUZRXRQSOCPSXKXNEHLQYKIBJRTMMHJOIZSWESTHTXPULAPGLZHBOLMP QWYSWWOGRJQGYWDWWZMHZMTDMRWBSPIXHCFFOHTJSOAULKIFZVXPTYEBTBEXGQNBQAECQOJGHTKIAXUJLSLPBKTTRORROLNTKPDPOMSZBBLUYF RZXYZSVBGBEMGTACDCBJNXKAMZMCYEWGKSUENLKBJSZIPKQGYXMJTJXBELNVMAZHRUESZSTWROIUXLLMQPYLVQYLCOMOCGPSMJQGILSDDRUUXD RUCCVECNPLWHJLTHCPBZIKDUNRJMJIOQOCHVVNIQFFXFKFHTCVEEAXHTLJMWIUAWAMHGIGQCQJZGXBEDCRRZCNVYKCPWVJCRXIGXZYJENNARSZ ZREAOODIGZVBXFPAHTZNKNQHLNNETJICOVQGFLQSGSLCOYMPYDSGOPNUXAMCIJBJPJBAABYHKBKWCUAXUHNOCSSTHZYJXPLMFVJQAJDDSNEVXL RUYEQEKUKUIAOQAQJMNLHOUFLFUDMCWRNYNNLOACVSDXDNNBOGQOYGOZTWUOFZYLZQXJEGPQNQFLLILMQUJLCLUOOAOAQRCWMGKH GFJRPSFVQPCSCUDFVYSGDQIHJWSUDEAMVIANGMMFSJJTPNRYYSJYDFLUXJZGSYAAUHOEPMQIZZRSZDCXHRCIPUERSVKWEBDJCXEWWKPAHBVZES VEWPJTYRBKLHQRRPGDGQPGTNNFRMWNTGWIZDBPSGFQDFZWTVLRAOKRBHWFHBPZUBSCFBAMHEWXUIUXMKHPOCNYWNKSRYBQKSUWJL JRNBFNMTDBSZDXVFSLPDQEDCNYELVD

C:\Users\user\AppData\Local\Temp\tmp7B4C.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690299109915258
Encrypted:	false
SSDEEP:	24:0C2jKPS/GeHBPaNDdBKW/PXAx+sTTqBVw8tk7Ll/csnfv:UWKPaNjKW/PwxfTixkY/cSfv
MD5:	F0D9DE697149ECBC1D88C7EA4841E5BD
SHA1:	06A2A47C12B3554397AA0C8F483411CAB366947D
SHA-256:	5BE0708B77E41FC490ECEC9CDFF20C9479FC857E47CC276D6F68C0895EA68FB2
SHA-512:	E9953E00241C3FB48E267F1A49E2C53FEE4240415C7A48FAD089742C6C4AA1C5A9CCFEE616FC91EB29C1C8252A3095163A515ABA96A1F0B41A8B12992969691
Malicious:	false
Preview:	EEGWXUHVUGUAGDCAESAKQJADEXSKGQOTKSMYVIQMWCXKMREFNGUJHWRPPFJWEQHLMDSTAHLHBQSXLRGVYEPBLZILRXLTPZSELULGEDFWQHJHNI HNCTGEIAAPQHNOFANJGPRIYVQSOFCGDPFBTNYILXIPYTWVOYXFUCEEQWZRPXFERZCPKKZAHOYWHFAYDMSXERUPTEZISMPADRFDIWGTWAXETEOP JYWDNGCDFFZUXZZSPZVIILCQXOFDOGUOSZYPXXVLSNAWWPHQGNSYQXOUOGPFDMDNPFUONUSGUOUKYHHGHFFZYEDSZVDRUEJKGSHEMJARIAEZZD BZJFCMNUJIHQFHGDONGFEZRYCZYIAOXAXGWENMTPOKNMZPJSZVCDZRZPFIIYHXITKZBLAJXANTSBCWIGABZKBTKDJRSTSKYORPMNGHCZWCLOVF PZBMYKBYDRXMFUQJDNWZFCVEOXPGJMBQZRUEOTLHEFHKDZLVFBXLUSXRAXKVLWGOWARAQZHIMTYBWKPLWNJFMLQVXGRMIGEIPZEIFBYZRYNEEZ HFMFOGMBEWLJPBXWVYHVEUKSKVKINVMDJKCSAOUXTMIHLOJXLTEKLKJDYABXRPKNGFOXISIFXHABTYQIPUCFNIJWNCTAFGYEIBCCNXPZQAGPHN NRICKSKCXWERLWTFSJWUSCBTVWSYUVWXJQHMSZYHAHYELYFPIBFZETDRPQBQHKMCXRRCAEYFIERXQZVCDZZBPQJJDQUDHKPMDBXPEBPFURYAPU WVWVJRWXHFXQGMVUGOILYXGFSMEFMKLBFACOSIKHHXRBRGYVIVAOTFNIIOQUZTHBZGOGPVUVYSYNHRKOADWYTLCNTHHCZYXXGFCXMFHZBZBCCM TYSROXNAHKABYAXPWRNKHCJYLAMQAUZBVJWHFXISFSKFXGFPDIOTITGPUETUYHRIXQOTIGEVDQWEBJVPDIUZVQFUBWREJIPSNXDGEKXKULZFHZ QHQXPMBIYA

C:\Users\user\AppData\Local\Temp\tmp7B4D.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6998645060098685
Encrypted:	false
SSDEEP:	24:FzrJLVfPTlXwAGfwXz0vRDC0aYECjYTixDXXwDyDFdJCSuHFF03T:FRLVHTlXwAGEoVCRYF0EDXgDVFHUj
MD5:	1676F91570425F6566A5746BC8E8427E
SHA1:	0F922133E2BEF0B48C623BEFA0C77361F6FA3900
SHA-256:	534233540B43C2A72D09DBF93858ECD7B5F48376B69182EDBCA9983409F21C87

C:\Users\user\AppData\Local\Temp\tmp7B4D.tmp	
SHA-512:	07D3CA8902964865FE9909054CF90DA1852678FBE58B1C0A8C2DBA2359A16DCBD43F23142D957DB9C1A8C2A1811EF4FEA74B0016A6F469538366B4FF01C8A14
Malicious:	false
Preview:	NVWZAPQSQLDLCZFLTMOWSKLFWOMMGYWWTZSPFFTDRHOTSSRKDGSJCIGMJJNKHMSAEMKBPGYCFVANNLUHHUMQOHINWJABNFIWWWZX JLCANQSKWMIWKPMVTCWFUMQBAGWZRWHRCMJDSNPGGGNECNQGPIZXLBIMLXMHDDXDKVYPEKRCNITDGJJNAEAATOVDDPBUDYWRPDYW ARJTFXBUUZABBVURIWKONIVMPCYVUBTOTCIJJVRWYUNYHAFJZUMVTOIXZGAVVNSRENTVPHFLSLFWBLPFQDMQCJIHRXSQOTPSPDZKXCRBHZXDQI ECBJTNIRGCACNADPHRWIVAWGPANEMHGPPPARWYWAOAHPWQLEGOBGVNWVBIFLAEOZYELRFOEZQCQIXCQBUKZGPOQFLHFLCFTYWBDGCWMDWICTIC WVZEAQNJOOVCGQZYTBBXQPEYFQMSMETMKKZMRGXXLCDXDEEEJKZAUNEWZONYMVVIZOWQRUQYNOEFMWEVWXFAZRHGHUXGAYODAXDN QONZPVBKRYIOLZJIYSHJSCEPYVMYISKJIWPKVGUQBNLZCUFGXBFZDDRGUMCLJGJPDAZKZLRMDSBFEJQYNNKTHBMJMUHVUOIVZRULJFFYIUMOHU GCJUYZGXKXNIWZUKRIYDZATEOXGMHUPOOBIHEEVPKQEZDDWJHKEKLNTMWMDCFDOYCCDOERYFZNFUDEHYXIBQAVVOHQNIEWZODOFZDFJSWYCJMW WOIZSCZSZBGOIFHRDBXHKMCCLSYNVVXYLWKXEKVHIZEBIBHWMXDXEGZDYWRROMYHTDQVCLXOGVHWHFNIDZOXWTTPAMAKJIYLNQIEDSCCTSBLPH TTGLCIYXXWIBXAGYBACOKOTPPBKACWQBYRTKFMCSSRYQNESLPTLSLCWCSLHOGHNCGUFWMYXDBUFSOKFIDUIBHTQJFIQTVZZVIZEWTBSHJWKQXG UWLFKNDUSKPDSMJNJJNEEOWEHOKTNZWRDNOXWJEK

C:\Users\user\AppData\Local\Temp\tmp7B4E.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.685942106278079
Encrypted:	false
SSDEEP:	24:e80g32tqxncx15PRgoZOZUxcz6oV0dh0dxiXMK:e87SH5Go0ZeuDufAiXMK
MD5:	3F6896A097F6B0AE6A2BF3826C813DFC
SHA1:	951214AB37DEA766005DD981B0B3D61F936B035B
SHA-256:	E6E3A92151EEE0FCDF549A607AE9E421E9BB081D7B060015A60865E69A2A3D60
SHA-512:	C7BD241F0E71DC29320CC051F649532FFF471B5E617B648CC495413587C06C236AFA4673A7BC77409E989260278CDEF49BDACA38BEB6AF65FEE74C563775B97
Malicious:	false
Preview:	PIVFAGEAAVVMYOKLIHAGVKQSIBRMIEBPKZHRSRYSYCTZASSEWGQLTFYPITGFBLIMOSZPCOYJLDMIKUYRMFZNOVAKNNFUFMFWAQZIZZSOHPUKTM EQKVMZGORRHHUAPAVEHNTRHFTCOWUQLMTXHFAASXNSJOMVEVZKIBTYUEOEAYWORCLXNWXMWVTCVFUJOOHJFVBTQGYSPLVNZVQAKY RWBXASIFOBPMFAPMAVEFPAYEVCHLKOVGMAFTDZYSFCRVFLUCDEZSALOPZIFCHRCOADKGTQMGRAQFQVFLPTIZCOVQGXVCITLOKGAEHQOUDVVLBL ANQIWAMALJXSPVCLVLGENZFIFSPDTQOOAOXTRKMORBXQQUMCVCGJNJNIYGXUUXANSJRSROPOUDFHQHUUMMRXDQWLRABBQAZENYVIBHRRHTGWSI VVUQDLCOQYLVPAUFYYHGIERJJLVMIHLHHCCGHRLMANSNVNAYHLENOWUETBHLULUXLDUIUWHDTSBTXYABZUPEVNUTYDIYOWXZQQWZTIKHRACSWY ILZGJJAYPXSWVAJEAMWRWUWIOONUGSOWTNWVILBTRYWXPSGGJYETTQICCTQMOORSZENPULBEQOBSNDWJHFGZOXAYRMRTCQAGZFKLTXQJCKKKJT XRIIVBYSWRFFSDWLAWEVZNFVJIYAKGOFIKGKPALYKLUSFUZNXBTTGJQARLJLEPNMUPZBHUFERZBUARRWLRQMAELUFJHXEPWKNEOUOFWRPCGUFY JEWTUPSXMLBAGQWILTIUMBXONDPOFUHNKJJKISPTLDQHMYGKSUZUEBYHKNHJUVSBOBSFQWTBGVEFNVAAKMXTORQQDIBVTWEQECBUJMCLMNPNRT KIKGQQLCBXEDYYHZALQNWVUKKTUNZMKPSISXIDNZZXVGUERMWOJYWVPNSTVVUORBONVDVVOSICVUMWTQLGBVUNLJTMTSZIJARQMRHCGASSVBBF IRIMTSICIANQBRVHJQBP

C:\Users\user\AppData\Local\Temp\tmpA937.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmpA938.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmpA938.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD23D.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmpD23E.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmpD23F.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmpD26F.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831

C:\Users\user\AppData\Local\Temp\tmpD26F.tmp	
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\tmpD29E.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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\tmpD29F.tmp	
Process:	C:\Users\user\Desktop\aVfFzvm8iR.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..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.500533830304246
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	aVfFzvm8iR.exe
File size:	226816

General

MD5:	6991603097a011d73b25213dba357b93
SHA1:	c7d00bf33525837fd841c1d3d4255304a2b34566
SHA256:	111d1312a6f53b62202bc1901a200fecf7ad434853036279fe73287f8877897a
SHA512:	4e371f11fe10c3c18cdd19421535ad00242e6d9246dc0cf0c47f46fb0919ef370b6830c852e4198c18dab927c23a9d68b9cfa862d72cc2c8dc2a53ec5b2383af
SSDEEP:	6144:cGpz7KFZCZCVpeaFOxElVLiqd2SsKVYNrS:cGpqCZCVuE3eqdmKn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L....._...

File Icon

Icon Hash:	8c9cbcccce8888e7

Static PE Info

General

Entrypoint:	0x401cf5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5FC2C20C [Sat Nov 28 21:33:00 2020 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:	cff62fa5d60c26268b201fcb5b9dc813

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x29fe0	0x2a000	False	0.926223028274	data	7.91447313445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2b000	0x31d2	0x3200	False	0.255859375	data	4.19963144088	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2f000	0x8557c	0x1e00	False	0.11875	data	1.32926027872	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xb5000	0x8020	0x8200	False	0.616466346154	data	6.0316287541	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
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 10:06:52.527592897 CEST	192.168.2.7	8.8.8.8	0x354b	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:06:52.563070059 CEST	192.168.2.7	8.8.8.8	0x7d4c	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 10:06:52.547383070 CEST	8.8.8.8	192.168.2.7	0x354b	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:06:52.582876921 CEST	8.8.8.8	192.168.2.7	0x7d4c	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: aVfFzvm8iR.exe PID: 2904 Parent PID: 5180

General

Start time:	10:06:16
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\aVfFzvm8iR.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\aVfFzvm8iR.exe'
Imagebase:	0x400000
File size:	226816 bytes
MD5 hash:	6991603097A011D73B25213DBA357B93
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: 00000001.00000002.358831451.000000000211C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000003.272708961.00000000005CE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.361464127.0000000003645000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.359419486.0000000002320000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.359783464.0000000002540000.00000004.00020000.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: 5228 Parent PID: 2904

General

Start time:	10:06:16
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