ID: 490251
Sample Name:
QH3hnrCD8x.exe
Cookbook: default.jbs
Time: 10:12:13
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

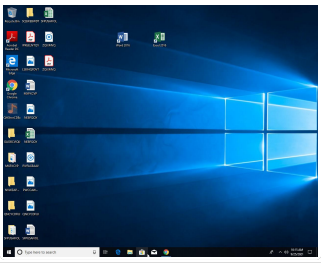
Windows Analysis Report QH3hnrCD8x.exe

Overview

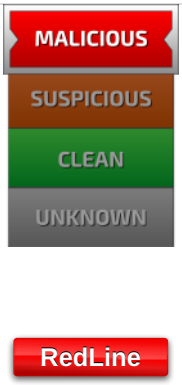
General Information

Sample Name:	QH3hnrCD8x.exe
Analysis ID:	490251
MD5:	4fa2f0b9cfd2544…
SHA1:	a43325c3a9208d..
SHA256:	555dd78ae57d3a..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

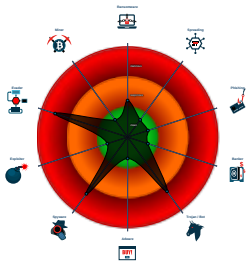


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …

Classification



Process Tree

- **System is w10x64**
- QH3hnrCD8x.exe (PID: 6848 cmdline: 'C:\Users\user\Desktop\QH3hnrCD8x.exe' MD5: 4FA2F0B9CFD2544D8ED9EC922E80A521)
  - conhost.exe (PID: 6864 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
00000000.00000002.778823967.0000000003795000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.776110627.0000000002450000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.775964863.000000000235C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.682820302.00000000006A7000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.775712248.00000000022F0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.QH3hnrCD8x.exe.22f0ee8.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.QH3hnrCD8x.exe.2450000.6.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.QH3hnrCD8x.exe.22f0000.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.QH3hnrCD8x.exe.22f0ee8.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.QH3hnrCD8x.exe.6a7970.1.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)

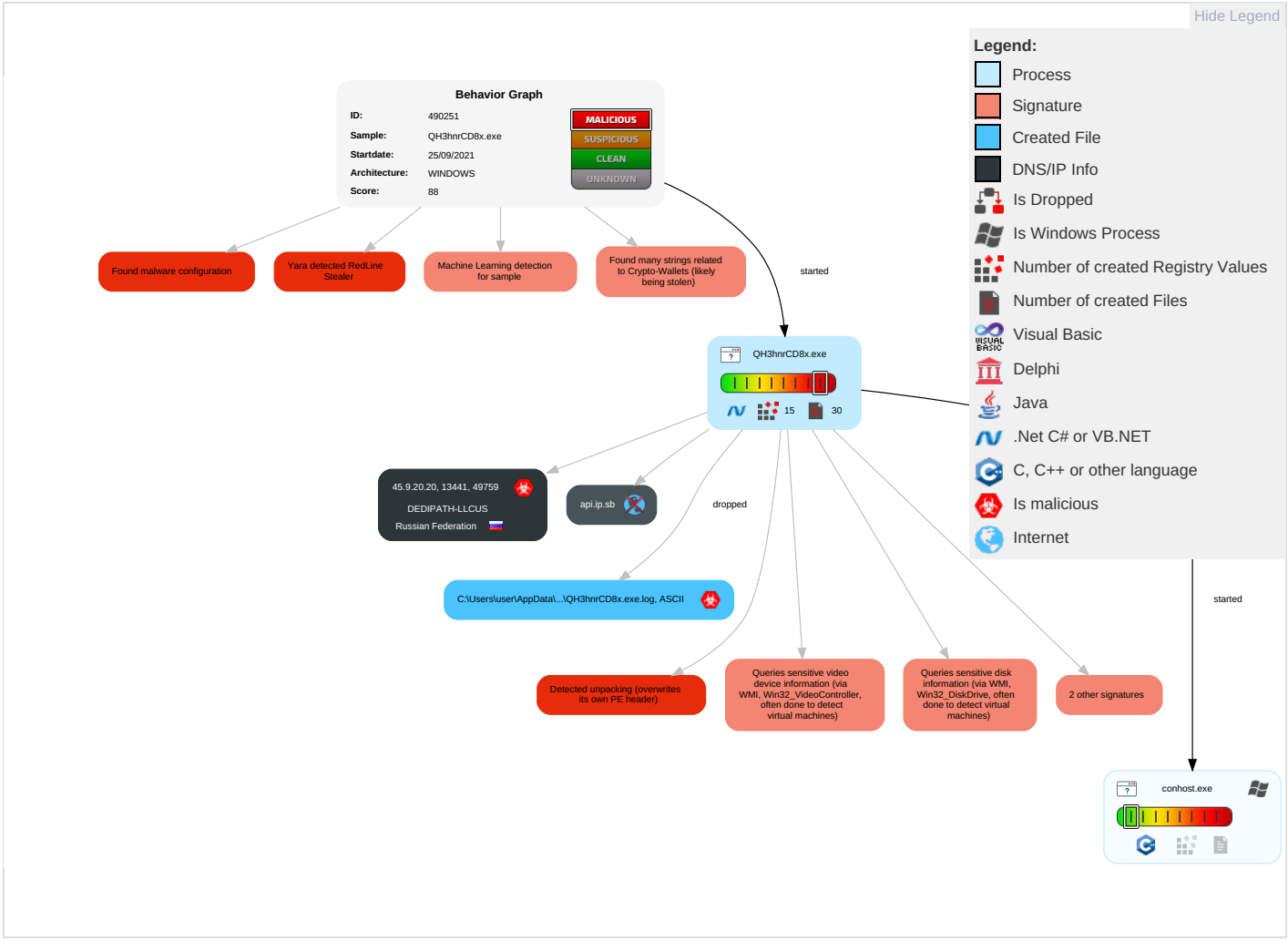
Remote Access Functionality:

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	Netwo 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

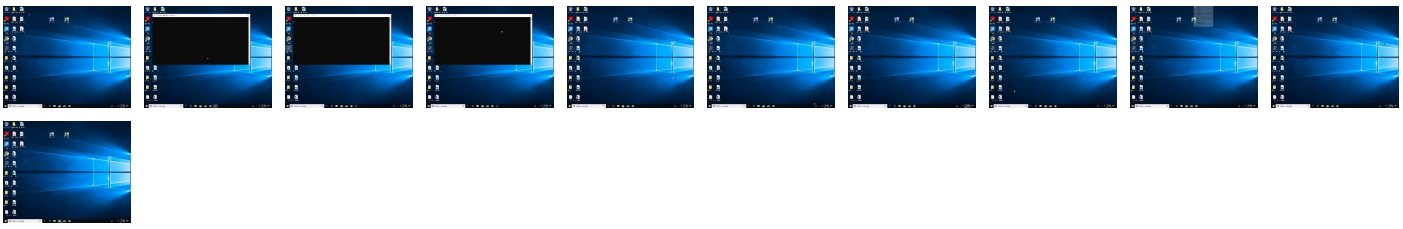
Behavior Graph



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
QH3hnrCD8x.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.QH3hnrCD8x.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Endpoint/PartInstalledSoftwares	0%	Avira URL Cloud	safe	
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	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490251
Start date:	25.09.2021
Start time:	10:12:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QH3hnrCD8x.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:	16
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@2/25@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6% (good quality ratio 5.8%) • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:13:47	API Interceptor	80x Sleep call for process: QH3hnrCD8x.exe modified

Joe Sandbox View / Context

IPs

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

Domains

No context

ASN

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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QH3hnrCD8x.exe.log	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKYHZHxLHG1qHqHs:Pqaq5qXAqLqdqUqzcGYqhQnoPtlxHbqU
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\tmp11E3.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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

C:\Users\user\AppData\Local\Temp\tmp11E3.tmp	
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\tmp1232.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp1233.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp323F.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp3240.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp3250.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp3251.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp514C.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.698669844484375
Encrypted:	false
SSDEEP:	24:7mMbmx9UKbA2JHc6cqYGtPrmwXr33hecYrnpTGwrhq0Lf6iNXQp:JI68rJcqjPSwXzRecYhGKq0LLG
MD5:	4FCF725C73B93BE52C2E1CD48AC3A562
SHA1:	98118BDED7CC2397C19310A914C6CA6B39CC47DE

C:\Users\user\AppData\Local\Temp\tmp514C.tmp	
SHA-256:	3803B68C31F1D6091C8D35F7B737B363C99ABED15B65899869E2A5AFA443D2C4
SHA-512:	8EDB10C8C81284109073EAABDB337F2AF5428AC5A50DE4999B61792D434D099124DF2DB5B2F58E9FC6335EA2E6F474291F8726DEF293A409418CDE6E0D5D7CF C
Malicious:	false
Preview:	MXPXCVPDVNZDMRYXKAXPKZSKXQENMVJGASOKSKKVKMVTFWCKJVQUEHFJLYGAGVTAPSEFWLYDESGESNCQQMFQIJOIYCFNJODSXZOERROXNDWXBZ RWZFOKQBPLORLXBDLECIGMCKVUGLWKNMZJBHPGARIQDCSYHCPUKBGABSYSPDCWIMLINBEYVYXKDRVQIRPITEAVGQTKEJGNRGJGNMXLAZZZEOVL CHVHUAHQLECFOLMZPDMGFZOZZRCUGUGQXZRQEEYVPMGAXSRCPXPOCBVPESPOAHTWHHDKCHMXTJCJJDRFYUOIUWGYDNCJXDYQFYCADMQIYTSLSI QVEMFCENTOHNQNWXMKIUOZDFCOFDXWRGCINHQCHYKQMLGTDJSTFEPKLURPPUWEFYLYEFPSNQGBKUZJQDAVMAFGFXHFNGMNUPXAYG ABBOYSAPGCMGQZYDGMRINVJWRFASDKOFXOQBOCWTMIFSMCIGFJLECWNXSPKYYMZPZTTKDCIUUBZTJKBGNEDOBUUIKPGSXPUUDSIAYBARDMCGXU VFSTYNWEUHFOSOADWNJSVGVNYVPTFIEGPCWGLEJGVLKBVQHFEPYYRMGWPMKQWLBOAFFRZQRDMFIHCLMXYKGCSNXZKWIKKIILSRZRKNKBMQKPDN BOSZDCMCNAMVOVGTUYRVJHPAMTCIPJHQZLFPQNHPQQTDAETXQMKGTZQPDKQISDDHIQFGGWJPCMAAAGGRYLKNAQHJDFVXQSDDSPCOTQDHQLRMFK VLQAFIBPIEJVVBHAMXWNJDJUFWZAUYOGKLIJAKPXHFCOGJJVGZXSWYIBAKNZMMSVHMHLNHNJCCWYZMEJWSAERLVHQEHUTACSGGGRMLAWNQTJDB BGLANCZUNRXUOYFLZHFFWFLDWPBOZWIRWKAIWLBOQNNKCSLPLMPBIDNPIJQEDKYXMBPUFPZCWHQURUYJBENNRMTLHPICTOSJUUPWITJRCCXDXE HQQYLVPFNZKWXNGEGYNB

C:\Users\user\AppData\Local\Temp\tmp514D.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696913287597031
Encrypted:	false
SSDEEP:	24:TEp0dGAR5tKV4V1dnQcncjGi20QoVwGQqh3:20Iw5tKOncjGUwra
MD5:	44ECF9E98785299129B35CBDBCAB909B
SHA1:	4D92AFB00FE614CC8B795F1AF28173DBE76FE7F5
SHA-256:	06E706536CB7D543E6068C98C90721CAD89C23D16D37444F46F9B01C4380DF9E
SHA-512:	1FA347223014BB3AC0106948B07E337B1A98C0BA2D98AC0ADD821D1B3CE9F75681F6383925F5E614F36750C5B9FB92D1C8EEEDC05469FBC6EA3F281D8B52B55 6
Malicious:	false
Preview:	SFPUSAFIOLDMTRNUTGNTJUWFCWSZSHWEDVXRKVRQQJURAYWLWUUBTIKENFOXKWAEIMQEIZNZNRADQPATZGCMDPRDXLQGZUFJZGZDRTSVNCHAUP MRLPRPZKGVAVXYEVCKEHKMMJGKSJOOUYGYLDDIEYHRSUUPROPBGJMTERPOAVKYFPSCESRJNQZFKBQPUDQDDUMCFWKLZTOAKIRCBYNHNUNDHQGU CZFGLFAWYRAYVDHRMGQXAXAOYSCNPGEKEPCMQBIHRFANOHHAWKRVIORZYSDKULQZFRPSGFVYRDRVLMMPKWJDXUOEBNLILNONKXLMXLVIUCYNNQ GCPDXMGSCUEKRTGZJHMNRUEKEIJFJIAHVLHOVPEFBBLWOKZSZSYSSOQIMAXYTLNUMGPOHCVAJUEBTRJRPRJCOTKTDCOEZCJXDLESVDTKVOFQWE NRQDQXACWTCILXCPGHHUNHJNQLPPCERJAOCZFIXIHZKTCKZMXYDXVVFZUURETLUVBDNYJHWBIGQTEBATUDWNJLGPYCGIXUBQTVJPDRWVOFIQDY MJOMWUQUNCHQWGETEEEIJZNHHUYACVFRBGSWATTYVHFTURPBDTDDQTWASRBMLCMLRKIGMHWRHHHUVZTGIFNIDBHRKNFOYFIOYERMIXFEIANSZH VUVBFJOQNNJGQUNDLTPKRMYXNUHBOFQLLIDRDFMIAAVQNNXFNDRFBIGEVUSBEJUVVSTEJYKSAUCFDNNJQTSVXAUBHAPFHJIYCNFJQPWEXKMUQR CKERPSFCQKHEDKHHRNWTLAMXHJLOSIZOKYIMDHNEIBAUBKXVXZVXMAZNFTTYQGDGZHKLIHZJNIVHVZHYMNESIMFITKHGIPXKXZDBLBTKTNZDKZ TKDHQQJCJDTRVKOCTCXPMDLKSOBGZSQQUTNFYYEOCJVZSZUSESOBKMIJSKKSXTXITISLBTMALAVZEMHXQXVRBZCDKLOKWDYQIEQCKFLKBMPLIQ MKDTJPRHOW

C:\Users\user\AppData\Local\Temp\tmp514E.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.698669844484375
Encrypted:	false
SSDEEP:	24:7mMbmx9UKbA2JHc6cqYGtPrmwXr33hecYrnpTGwrhq0Lf6iNXQp:JI68rJcqjPSwXzRecYhGKq0LLG
MD5:	4FCF725C73B93BE52C2E1CD48AC3A562
SHA1:	98118BDED7CC2397C19310A914C6CA6B39CC47DE
SHA-256:	3803B68C31F1D6091C8D35F7B737B363C99ABED15B65899869E2A5AFA443D2C4
SHA-512:	8EDB10C8C81284109073EAABDB337F2AF5428AC5A50DE4999B61792D434D099124DF2DB5B2F58E9FC6335EA2E6F474291F8726DEF293A409418CDE6E0D5D7CF C
Malicious:	false
Preview:	MXPXCVPDVNZDMRYXKAXPKZSKXQENMVJGASOKSKKVKMVTFWCKJVQUEHFJLYGAGVTAPSEFWLYDESGESNCQQMFQIJOIYCFNJODSXZOERROXNDWXBZ RWZFOKQBPLORLXBDLECIGMCKVUGLWKNMZJBHPGARIQDCSYHCPUKBGABSYSPDCWIMLINBEYVYXKDRVQIRPITEAVGQTKEJGNRGJGNMXLAZZZEOVL CHVHUAHQLECFOLMZPDMGFZOZZRCUGUGQXZRQEEYVPMGAXSRCPXPOCBVPESPOAHTWHHDKCHMXTJCJJDRFYUOIUWGYDNCJXDYQFYCADMQIYTSLSI QVEMFCENTOHNQNWXMKIUOZDFCOFDXWRGCINHQCHYKQMLGTDJSTFEPKLURPPUWEFYLYEFPSNQGBKUZJQDAVMAFGFXHFNGMNUPXAYG ABBOYSAPGCMGQZYDGMRINVJWRFASDKOFXOQBOCWTMIFSMCIGFJLECWNXSPKYYMZPZTTKDCIUUBZTJKBGNEDOBUUIKPGSXPUUDSIAYBARDMCGXU VFSTYNWEUHFOSOADWNJSVGVNYVPTFIEGPCWGLEJGVLKBVQHFEPYYRMGWPMKQWLBOAFFRZQRDMFIHCLMXYKGCSNXZKWIKKIILSRZRKNKBMQKPDN BOSZDCMCNAMVOVGTUYRVJHPAMTCIPJHQZLFPQNHPQQTDAETXQMKGTZQPDKQISDDHIQFGGWJPCMAAAGGRYLKNAQHJDFVXQSDDSPCOTQDHQLRMFK VLQAFIBPIEJVVBHAMXWNJDJUFWZAUYOGKLIJAKPXHFCOGJJVGZXSWYIBAKNZMMSVHMHLNHNJCCWYZMEJWSAERLVHQEHUTACSGGGRMLAWNQTJDB BGLANCZUNRXUOYFLZHFFWFLDWPBOZWIRWKAIWLBOQNNKCSLPLMPBIDNPIJQEDKYXMBPUFPZCWHQURUYJBENNRMTLHPICTOSJUUPWITJRCCXDXE HQQYLVPFNZKWXNGEGYNB

C:\Users\user\AppData\Local\Temp\tmp517D.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696913287597031

C:\Users\user\AppData\Local\Temp\tmp517D.tmp	
Encrypted:	false
SSDEEP:	24:TEp0dGAR5tKV4V1dnQcncjGi20QoVwGQqh3:20Iw5tKOncjGUwra
MD5:	44ECF9E98785299129B35CBDBCAB909B
SHA1:	4D92AFB00FE614CC8B795F1AF28173DBE76FE7F5
SHA-256:	06E706536CB7D543E6068C98C90721CAD89C23D16D37444F46F9B01C4380DF9E
SHA-512:	1FA347223014BB3AC0106948B07E337B1A98C0BA2D98AC0ADD821D1B3CE9F75681F6383925F5E614F36750C5B9FB92D1C8EEEDC05469FBC6EA3F281D8B52B55 6
Malicious:	false
Preview:	SFPUSAFIOLDMTRNUTGNTJUWFCWSZSHWEDVXRKVRQQJURAYWLWUUBTIKENFOXKWAEIMQEIZNZNRADQPATZGCMDPRDXLQGZUFJZGZDRTSVNCHAUP MRLPRPZKGVAVXYEVCKEHKMMJGKSJOOUYGYLDDIEYHRSUUPROPBGJMTERPOAVKYFPSCESRJNQZFKBQPUDQDDUMCFWKLZTOAKIRCBYNHNUNDHQGU CZFGLFAWYRAYVDHRMGQXAXAOYSCNPGEKEPCMQBIHRFANOHHAWKRVIORZYSDKULQZFRPSGFVYRDRVLMMPKWJDXUOEBNLILNONKXLMXLVIUCYNNQ GCPDXMGSCUEKRTGZJHMNRUEKEIJFJIAHVLHOVPEFBBLWOKZSZSYSSOQIMAXYTLNUMGPOHCVAJUEBTRJRPRJCOTKTDCOEZCJXDLESVDTKVOFQWE NRQDQXACWTCILXCPGHHUNHJNQLPPCERJAOCZFIXIHZKTCKZMXYDXVVFZUURETLUVBDNYJHWBIGQTEBATUDWNJLGPYCGIXUBQTVJPDRWVOFIQDY MJOMWUQUNCHQWGETEEEIJZNHHUYACVFRBGSWATTYVHFTURPBDTDDQTWASRBMLCMLRKIGMHWRHHHUVZTGIFNIDBHRKNFOYFIOYERMIXFEIANSZH VUVBFJOQNNJGQUNDLTPKRMYXNUHBOFQLLIDRDFMIAAVQNNXFNDRFBIGEVUSBEJUVVSTEJYKSAUCFDNNJQTSVXAUBHAPFHJIYCNFJQPWEXKMUQR CKERPSFCQKHEDKHHRNWTLAMXHJLOSIZOKYIMDHNEIBAUBKXVXZVXMAZNFTTYQGDGZHKLIHZJNIVHVZHYMNESIMFITKHGIPXKXZDBLBTKTNZDKZ TKDHQQJCJDTRVKOCTCXPMDLKSOBGZSQQUTNFYYEOCJVZSZUSESOBKMIJSKKSXTXITISLBTMALAVZEMHXQXVRBZCDKLOKWDYQIEQCKFLKBMPLIQ MKDTJPRHOW

C:\Users\user\AppData\Local\Temp\tmp523E.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp523F.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp5240.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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

C:\Users\user\AppData\Local\Temp\tmp5240.tmp	
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5241.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp5242.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp5272.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp5273.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp5274.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp737A.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp737B.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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

C:\Users\user\AppData\Local\Temp\tmp737B.tmp	
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp737C.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmp737D.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.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\tmpF179.tmp	
Process:	C:\Users\user\Desktop\QH3hnrCD8x.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.494367603050098
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:	QH3hnrCD8x.exe
File size:	227328
MD5:	4fa2f0b9cfd2544d8ed9ec922e80a521
SHA1:	a43325c3a9208d6cdfae0cbd082cda652d03ec63
SHA256:	555dd78ae57d3a34f8c9bf6a4c896dbc765454ab6eaa12c84ea9631301c97be1
SHA512:	b1d40d9872154ce8824b65264559e9073258da160da98f1538b23f3811ea33a75627b2f824a65850fc004641d44e5c503618e4a4c60e2137a1812294655990de
SSDEEP:	3072:5B+CvVzj+8mw8z/g5zfQUgtvbJVEc0/a1/XPi5hcaLzucn3K/D5eALyGIGRY5:5B+OzjXQqzfQlt6c71yr7nTn3qfNR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L...&i._...

File Icon

Icon Hash:	8c8cbcccce888ae7

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, NX_COMPAT
Time Stamp:	0x5FEA6926 [Mon Dec 28 23:24:22 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	0x2a0d0	0x2a200	False	0.924871337166	data	7.90958495865	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x2c000	0x31d2	0x3200	False	0.254453125	data	4.1909884481	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x30000	0x8557c	0x1e00	False	0.118229166667	data	1.33309239879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x8020	0x8200	False	0.617127403846	data	6.03555904278	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
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:13:47.190563917 CEST	192.168.2.4	8.8.8.8	0x3a12	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:13:47.765388966 CEST	192.168.2.4	8.8.8.8	0x81c7	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:13:30.683166027 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:13:47.210179090 CEST	8.8.8.8	192.168.2.4	0x3a12	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:13:47.788778067 CEST	8.8.8.8	192.168.2.4	0x81c7	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: QH3hnrCD8x.exe PID: 6848 Parent PID: 5536

General

Start time:	10:13:10
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\QH3hnrCD8x.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QH3hnrCD8x.exe'
Imagebase:	0x400000
File size:	227328 bytes
MD5 hash:	4FA2F0B9CFD2544D8ED9EC922E80A521
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: 00000000.00000002.778823967.0000000003795000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.776110627.0000000002450000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.775964863.000000000235C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.682820302.00000000006A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.775712248.00000000022F0000.00000004.00020000.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: 6864 Parent PID: 6848

General

Start time:	10:13:11
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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