ID: 490263
Sample Name:
5hOpZFd0b4.exe
Cookbook: default.jbs
Time: 10:24:23
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 5hOpZFd0b4.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: RedLine 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Compliance: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 11
Created / dropped Files 11
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 18
Rich Headers 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Possible Origin 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 18
DNS Queries 18
DNS Answers 19
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: 5hOpZFd0b4.exe PID: 4668 Parent PID: 3976 19
General 19
File Activities 19
File Created 20
File Deleted 20
File Written 20

File Read 20
Registry Activities 20
Analysis Process: conhost.exe PID: 800 Parent PID: 4668 20
General 20
Disassembly 20
Code Analysis 20

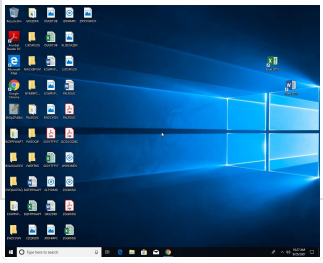
Windows Analysis Report 5hOpZFd0b4.exe

Overview

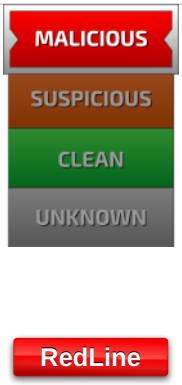
General Information

Sample Name:	5hOpZFd0b4.exe
Analysis ID:	490263
MD5:	a6be05bdc87a77..
SHA1:	474993b69aa3f2c.
SHA256:	e5ca91a98799cc...
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

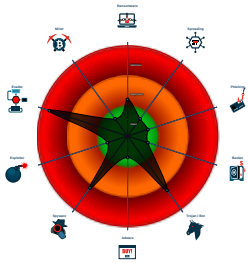


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm...
- Detected unpacking (overwrites its o...
- Detected unpacking (changes PE se...
- Machine Learning detection for samp...
- Queries sensitive video device inform...
- Queries sensitive disk information (v...
- 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**
- 5hOpZFd0b4.exe (PID: 4668 cmdline: 'C:\Users\user\Desktop\5hOpZFd0b4.exe' MD5: A6BE05BDC87A77421C9EF0834488071D)
  - conhost.exe (PID: 800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "185.215.113.29:18087"
  ],
  "Bot Id": "SewPalpadin"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.333679993.0000000004A0C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.333955560.0000000004BD0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.333573103.00000000049A0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.252716229.0000000002EF9000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.336091317.0000000005E95000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.5hOpZFd0b4.exe.2ef9c90.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.5hOpZFd0b4.exe.4a4d896.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.5hOpZFd0b4.exe.2ef9c90.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.5hOpZFd0b4.exe.4a4c9ae.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.5hOpZFd0b4.exe.49a0ee8.2.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 harvest and steal browser information (history, passwords, etc)

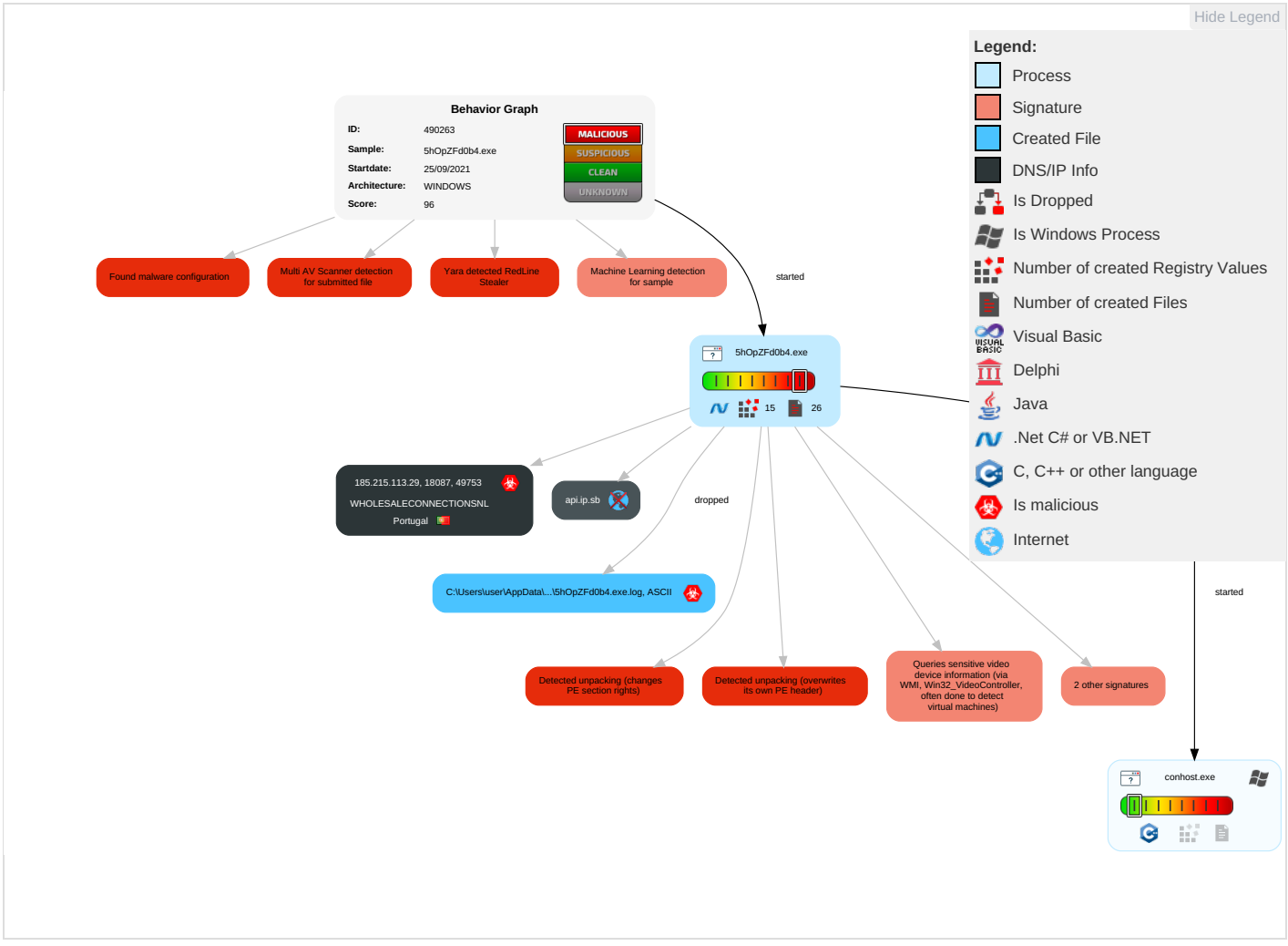
Remote Access Functionality:

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 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 Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 1 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

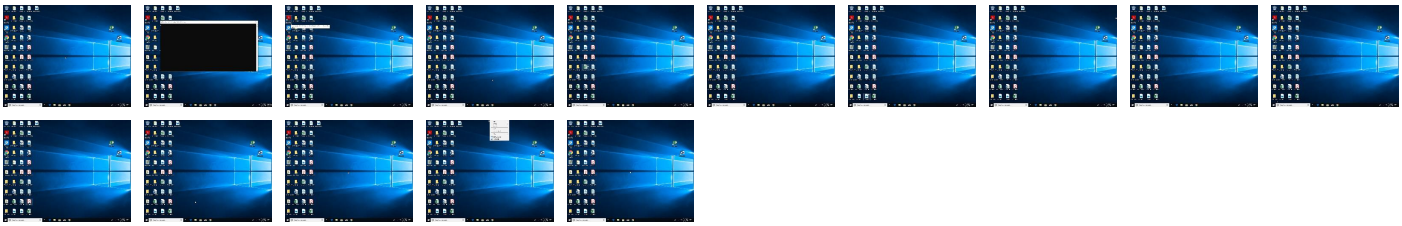
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
5hOpZFd0b4.exe	31%	Virustotal		Browse
5hOpZFd0b4.exe	43%	Metadefender		Browse
5hOpZFd0b4.exe	62%	ReversingLabs	Win32.Trojan.Racealer	
5hOpZFd0b4.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ip.sb/geoip%USERPEnviron	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartInstalledSoftwares	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartNordVPN	0%	Avira URL Cloud	safe	
http://tempuri.org/	2%	Virustotal		Browse
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	
http://tempuri.org/Endpoint/PartProcesses	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/InitDisplayResponse	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
185.215.113.29	unknown	Portugal		206894	WHOLESALECONNECTION SNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490263
Start date:	25.09.2021
Start time:	10:24:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5hOpZFd0b4.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:	23
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:	mal96.troj.spyw.evad.winEXE@2/21@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.2% (good quality ratio 16.4%) • Quality average: 82.9% • Quality standard deviation: 26.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:25:56	API Interceptor	57x Sleep call for process: 5hOpZFd0b4.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.215.113.29	D6SC0XwBgv.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	FuoEIkw29J.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	1DRClVcvyg.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	Vjbf4PaYXu.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	EcCFvo5Yg3.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cZkvTVcizO.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	QmQBacnCTx.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	qBl2sJ5hXX.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	MOo5ZnFWlk.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	O202OlZmVw.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	J3xXakZOIk.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	V1yj2IcuOo.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	pPuQoDVlk3.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	17IEkKetFQ.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	C4AKzpYmot.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	VJSiJkzclz.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	ujwlH05f2J.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	WzqeTOeBaS.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	8jMAwOsdLf.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/
	0bLwEL9k0P.exe	Get hash	malicious	Browse	• 185.215.113.29:8889/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WHOLESALECONNECTIONSNL	KqXA36ARxD.exe	Get hash	malicious	Browse	• 185.215.113.104
	jfTy8Hld20.exe	Get hash	malicious	Browse	• 185.215.113.205
	WydlYoRoDE.exe	Get hash	malicious	Browse	• 185.215.113.15
	yxHYlyS6ec.exe	Get hash	malicious	Browse	• 185.215.113.205
	IocDW5lw8k.exe	Get hash	malicious	Browse	• 185.215.113.205
	qUaCp2QNnD.exe	Get hash	malicious	Browse	• 185.215.113.77
	DHL.exe	Get hash	malicious	Browse	• 185.215.113.102
	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 185.215.113.104
	2Ft1sMVv6a.exe	Get hash	malicious	Browse	• 185.215.113.104
	awele.exe	Get hash	malicious	Browse	• 185.215.113.102
	XMmIpHPGeS.exe	Get hash	malicious	Browse	• 185.215.113.15
	sZqcv9vi4c.exe	Get hash	malicious	Browse	• 185.215.113.15
	SetupPro_D1.exe	Get hash	malicious	Browse	• 185.215.113.104
	SetupPro_D1.exe	Get hash	malicious	Browse	• 185.215.113.104
	02xPQm5RPL.exe	Get hash	malicious	Browse	• 185.215.113.17
	JskvQ68BCj.exe	Get hash	malicious	Browse	• 185.215.113.29
	RP1LeoZ1yS.exe	Get hash	malicious	Browse	• 185.215.113.15
	yVel5pTl3G.exe	Get hash	malicious	Browse	• 185.215.113.77
	1fZWE7rohE.exe	Get hash	malicious	Browse	• 185.215.113.104
	KVEFe5ARZG.exe	Get hash	malicious	Browse	• 185.215.113.29

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5hOpZFd0b4.exe.log	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmp79C9.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmp79CA.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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

C:\Users\user\AppData\Local\Temp\tmp79CA.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp9FD1.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmp9FD2.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpC58B.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpC58C.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpC58C.tmp	
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\tmpC5CC.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmpC5CD.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmpEA3.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEA3.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEA4.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEA7D.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEA7E.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEAAD.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpEAAD.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\tmpEAAE.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEB4.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEB5.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEB5.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEB6.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEF6.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEF7.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.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\tmpEF8.tmp	
Process:	C:\Users\user\Desktop\5hOpZFd0b4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\tmpEF8.tmp	
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.366376211223636
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:	5hOpZFd0b4.exe
File size:	390144
MD5:	a6be05bdc87a77421c9ef0834488071d
SHA1:	474993b69aa3f2cb09853e58c55975e9ec16653a
SHA256:	e5ca91a98799cc7a0fdcd0c45f0fce3bfc03ac7d77a7dd20874d6ac5b6476085
SHA512:	20fb503f9d7b5723e9342f563d6c7fd2684d8f4b0e7ce2ef45a6f19befd920bf057c42ff36b73dde52e4c523a4c872842fbc76d3b9e3a91bdbfefc3bc840392b
SSDEEP:	6144:s5R/5dPHRdH+eFDiaBVm9/UWCOR7JsNFLwM48u7nut6P4+QWBsJI:s55dPHRdH3Fo9/eo7ucTg+FII
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}*..9K..9K..9K..'...(K..'...UK..'....K.....<K..9K...K..'...8K..'...8K..'...8K..Rich9K.....PE..L.....^...

File Icon

Icon Hash:	aedaae9ec6a68aa4

Static PE Info

General

Entrypoint:	0x401cc0
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:	0x5ED1F089 [Sat May 30 05:35:05 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5

General

OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	0f0c12643909b692a9be3510bdc965e8

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1b960	0x1ba00	False	0.454866020928	data	6.27207258835	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x86cc	0x8800	False	0.299373851103	data	4.74825267165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x26000	0x276875c	0x23800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x278f000	0x3f68	0x4000	False	0.65478515625	data	5.82456093334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2793000	0x134d0	0x13600	False	0.0702620967742	data	0.910567807007	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

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:25:55.700730085 CEST	192.168.2.5	8.8.8.8	0x1951	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:25:55.739392996 CEST	192.168.2.5	8.8.8.8	0x4e74	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)

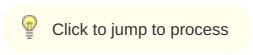
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:25:55.724314928 CEST	8.8.8.8	192.168.2.5	0x1951	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:25:55.761879921 CEST	8.8.8.8	192.168.2.5	0x4e74	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 5hOpZFd0b4.exe PID: 4668 Parent PID: 3976

General

Start time:	10:25:23
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\5hOpZFd0b4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5hOpZFd0b4.exe'
Imagebase:	0x400000
File size:	390144 bytes
MD5 hash:	A6BE05BDC87A77421C9EF0834488071D
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: 00000000.00000002.333679993.0000000004A0C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.333955560.0000000004BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.333573103.00000000049A0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.252716229.0000000002EF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.336091317.0000000005E95000.00000004.00000001.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: 800 Parent PID: 4668

General

Start time:	10:25:24
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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