ID: 490247
Sample Name: 6UclBifP3f.exe
Cookbook: default.jbs
Time: 10:05:06
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

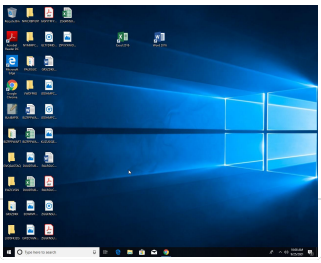
Windows Analysis Report 6UclBifP3f.exe

Overview

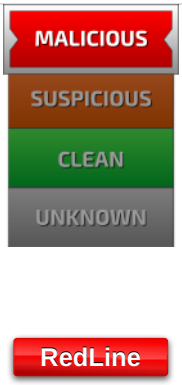
General Information

Sample Name:	6UclBifP3f.exe
Analysis ID:	490247
MD5:	1adb2662c75187..
SHA1:	50334d8144ca82..
SHA256:	e620189fa4c882f..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

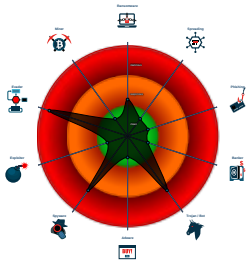


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Wallets
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- 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**
- 6UclBifP3f.exe (PID: 3372 cmdline: 'C:\Users\user\Desktop\6UclBifP3f.exe' MD5: 1ADB2662C75187EF4AAD7BE7F16A8F4D)
  - conhost.exe (PID: 2248 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
00000000.00000002.402230300.0000000005E15000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.396975534.0000000004DE0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.395986015.00000000048C0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.315015554.0000000002E8B000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.396296874.00000000049AC000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.6UclBifP3f.exe.49ed876.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.6UclBifP3f.exe.48c0000.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.6UclBifP3f.exe.49ed876.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.6UclBifP3f.exe.49ec98e.5.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.6UclBifP3f.exe.48c0ee8.2.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

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

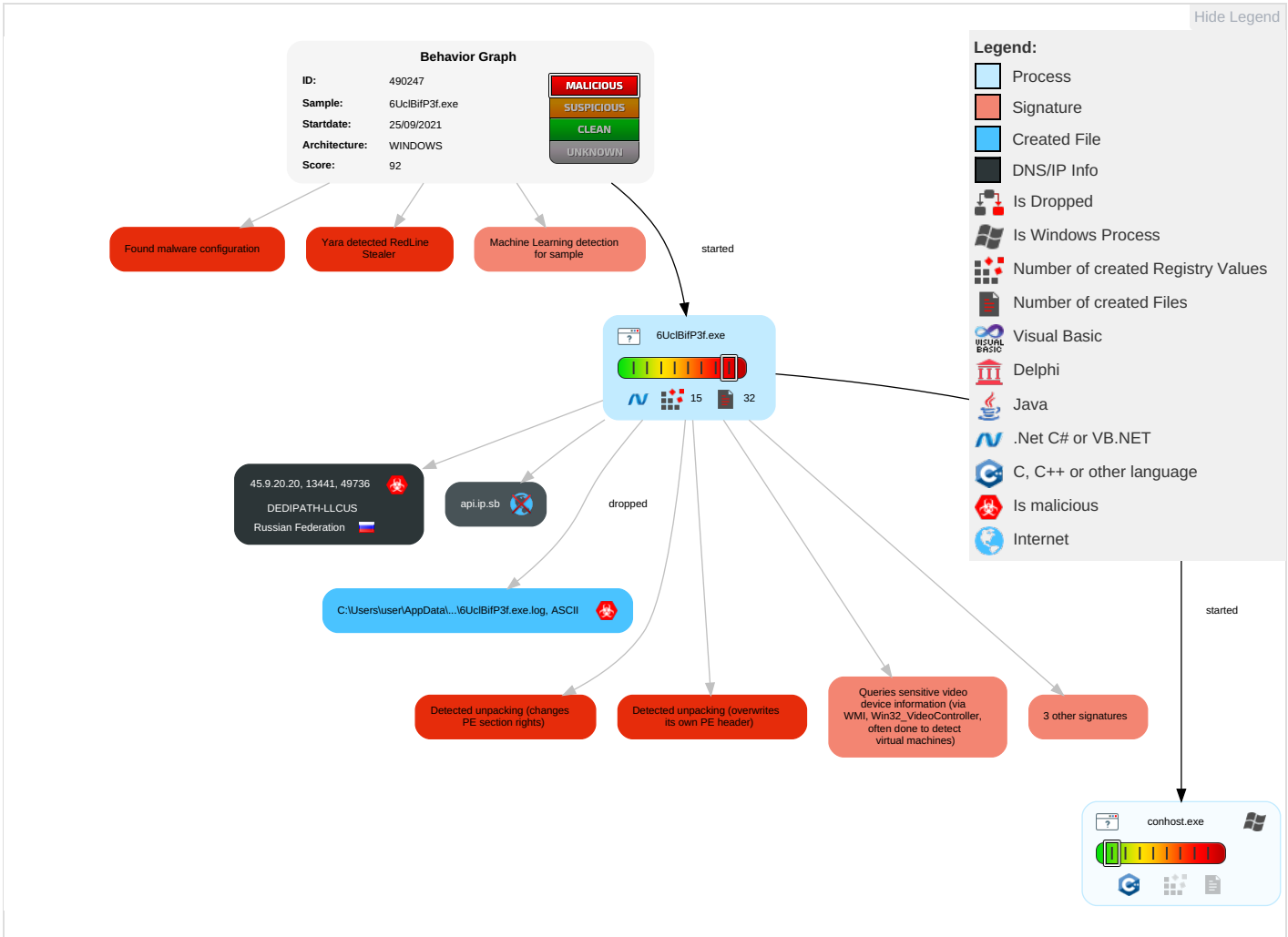
Remote Access Functionality:

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 Effect
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 2 6 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Local System 2	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 Comm
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
6UclBifP3f.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Endpoint/PartInstalledSoftwares	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartNordVPN	0%	Avira URL Cloud	safe	
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:	490247
Start date:	25.09.2021
Start time:	10:05:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6UclBifP3f.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:	22
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:	mal92.troj.spyw.evad.winEXE@2/27@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.4% (good quality ratio 18.7%) • Quality average: 84.4% • Quality standard deviation: 24.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:06:42	API Interceptor	62x Sleep call for process: 6UclBifP3f.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	
	vrZJf2r6Mz.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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\6UclBifP3f.exe.log

Process:	C:\Users\user\Desktop\6UclBifP3f.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6UclBifP3f.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\tmp487F.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp4880.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp68FA.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp68FB.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp68FC.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp68FD.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp693C.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85

C:\Users\user\AppData\Local\Temp\tmp693C.tmp	
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Temp\tmp693D.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Temp\tmp8969.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp896A.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmp896B.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\tmp896B.tmp	
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp896C.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmpA8AD.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmpA8BD.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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

C:\Users\user\AppData\Local\Temp\tmpA8BD.tmp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpA8BE.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmpA8BF.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmpC544.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861DC
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpC544.tmp	
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\tmpC545.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697358951122591
Encrypted:	false
SSDEEP:	24:GllFjmGrUw8wsY1UbsUhBRShwdYjDuvHNeGXNei:WFewtsZZp8DkHzNL
MD5:	244A1B624BD2C9C3A0D660425CB1F3C6
SHA1:	FB6C19991CC49A27F0277F54D88B4522F479BE5F
SHA-256:	E8C5EAACF4D2C4A65761719C311785A7873F0B25D849418ED86BBFE9D7F55C96
SHA-512:	9875E6DE2ACC859CACC2873F537DDE6ED4EC8CA00CBA3D28535E0440D76FFD475B66C52B6217D311D301C4B9A097619CF29A26B2FD54D03CD27A20A17EC9C 31
Malicious:	false
Preview:	GRXZDKKVDBUGJWVAVQNLKHTVWJFMWUAIFGXJYDZTDDYOZYAHDDDHNXHNVSFVZJEMKSJXGDABHWXKQZCQXBMLFZCFZRGZPZWYYNETLMDWOLDLPI FOVKRDMQEWUEHKITHNGNRTRZWQHFMBDECTTQKFDEVNVHBAPCNMCJNWWITPVACWBIUNPCYFZKGJXCMBWDNHDCVDCGEKHYPPPEGKPC PMYZEKRCOGRHDFANVZFDZEKZWOKLRIOUPCTJCKQPECVEEGNTLJWZOKHSKZRNLJEDQLEQNRWIYLSXHSNVGFTCDJOFJSSGANZFCFSTDUPYBCCAPQ WVVVHWQMAMBVDQNABQSQOSDYDMOVPXENCAXSTPDCENIQOWPCOQHPSISEOWFKMBLGAZRALPTAYHDZLKJTCHXGTPXNIVUMCOJRZXPU VUFPCWEAEZMMLATLTGHPJIMHWFBUWIATNBBPFGVFXNULJLRYLAGRNCKVAJADSLQGVLGIYOHDIWUERAQSCTFBMXCMLCXSHZGTWPBCVHUYPVAFSB ZNBGAGMHGULJYULEEHPGNBGEQRAOPBXXMZIUIPJMFAOVNMZZTOZGOZOJPKWCEFTTAVUBAADATZYJDWSZEZPLDTGYCYWTSDQTIMZHCKMQLZFEYS YUUWFJSYEFNDDKQMZVTBOZLQBDKFHMMKIYQPFKZLTSHIJVNPHPCTWBWPTTKDHDZEMDVWXXBLPWLCSSBMTLIVOVYOKQCJKTYJWGJUBQUGQVBYJQ QLLGTHWSPFLDMDWBTOQUISHXBCHIJKAJFIPBNKMWVQGUSJVNKXAXFDNOBYJXMWRDAZWUJSRMMFQXDPYYKOFBEROBQMDZHDZZHOEIOKDOCHQQDQ QRHOROOIFAGQEJZJFZIGPJIRWVNQYZAJAHAWIEFFNXLXQWIUWYSGZDFYPCCGWYBBFQQMSMJBRIUPFBWIHWJWVCYOBNNXKIIWTIXOWRVLFBGPGW FQTGPUNWKWUUMQXIKNCLTTGYHBMKXJ

C:\Users\user\AppData\Local\Temp\tmpC575.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696508269038202
Encrypted:	false
SSDEEP:	24:RSjVGe9uHEleifrd16Wa05tSl2jFQzpqPMXexMApqIjsp:2Ge9MQ/d16Wjtc2j64Phxjpq82
MD5:	0E9E92228B27AD7E7B4449467A529B0C
SHA1:	209F92CDFC879EE2B98DEF315CCE166AFEC00331
SHA-256:	284937D0EBFEDD95B2347297D957320D8D5CA5FC48218296767069CABA6B14A6
SHA-512:	CECA5F634268817B4A076414FFAB7D81F93EEC7E7D08B8691CCE0B2BCAF8FC694365455886E36983B4D8D758BC65BC1868BE8DB51AD41E082473726BB1FFD7 8
Malicious:	false
Preview:	PALRGUCVEHIRKBYGKJJWKNMNYKFUTLHCEDOTKTWJCZHNZMOUNMNREQTGFDNZTATQQPDFONRIRAZYJEPXQVIVWNBDQIMKULZMUINYTVUPNMQBQQ YLGCAJYFEIWZTWGYTHEJPFBRNGCTANCYOISUQMRINVDUEIROITGPJZCCOVCZIZBHLYBDARSNRLEOQQDWOSMHXNRNBXNWMRVAQZUASARYHEITVT VSLHRGBYURPTEUNAUCYMZTXOZXKDXUEUUVTNGWGSBRAWIJZDVZDLMZBKEVESROLUEDPITQGUXFSRFAVNSESAFZLNXMXUYRFUEUKCMNFITMUQEW TCKEGDPOXHJSXBDLFIOLLHDYIVOQVEYJEZMDIOFXZFCPXJEQLPCSHKUGRQKXAUMKTHUMHWFQZRGBRZHGHYRXRODJXEBANQHOOVFBZXKJHDCAAK HZGSWGKGEDWOOCFCEYHPAQBYBKRXOTJWSCPMRDXNRYAQFQHSHOFCHWJDKTFHACROGLPZFWDCIBJSUTMTRHJKEGAHSBAQLDTWPTXB LVYYBNJBKDUNGOUDVWZOBKOJKSMZERYOYBNMDSYUPHFDPUXOMKCYNSEBJHJVXSWTIMBDLPWYMYMQKYICPQEWMYDUMYJRSVQHDEELUFOEQYUIZB TNUNJNZQTDTIJKNOJNFJDDGEYVGDXTQINCQDGJRRPOBRUHQLMKFJSSNNCQMDHWQYMHWIBVNPHRQCBTMYBSOJYXCUAYTWUDETCJTTEQSPXKTRSQ BDJYENXLXJTQIYOZHEFAQOFBXKATTASAWEYGDPTTLZDAFVKRYLRNFSWZYBGUMRHHMNPVCVECBEVWEXNMSCXSGJRAQKAYEIULWHXXFKTJWPDMYU AOSFBKCTNCTQQXTLXIIJKYOPYBMSFGYLZDGOXTVIHYLUMJCRDRQXFLBDAUXBTNAPMACHVQILKZSQLNPPJVGXAXUMTOUMJJJYJSPJALITYYHOOM VVOQNOSSPBLMRBWWPYXB

C:\Users\user\AppData\Local\Temp\tmpC576.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.704346314649071
Encrypted:	false
SSDEEP:	24:XPzUwxdkbbeZScSZIv3ZoJNWhjcfzkabZsHx:fzUwx4bK+W/+fzuR
MD5:	8B66CD8FCBCEB253D75DB5CDE6291FA2

C:\Users\user\AppData\Local\Temp\tmpC576.tmp	
SHA1:	6CE0386190B9753849299B268AA7B8D15F9F72E2
SHA-256:	51AD0E037F53D8EEDFEBC58112BDFA30796A0A56FBD31B65384B41896489BDB4
SHA-512:	7C46027769E82ACD4E3ACB038FB80E34792E81B0527AE318194FE22BD066699A86E9B3E55AC5A1BCAC005FE0E8B7FB70B041656DF78BF84983A97CEDAA8861D C
Malicious:	false
Preview:	BJZFPPWAPTZISGUNDSDXEATFCUXAGEFCTTZKBNFYFVKDZEMPHZAJNCAVKZWYYNTVOWAJJLGAAUTHJTXJTGQLSVTGXPQIMVSAZAKJXHFSFGEVOJ UYTICTQZLJZDQYBUBYFSZSBIOBVSAJCHKIQYCAYMMOZZQCCHGYUFOUMXHXCPNMUMVVZRXZCGPDXYDBBMVMWVPHNHLTQKLDBALGGHIVJYUKXJWA FDLMMQQUEQFWPXRQQODUGQSALTDJTROBSIRXEJYUMIWWHBCANDJZNUJGIKFXUWXKPWKATRJSISRBLFZRNYVGGJJMECDAMBUVQBAZGLVITWWCNZ FHKZSKXZCMBCAKDDJCKKLPSOZVUJSWOYBBVEUPDSCKJRFEYGLDGCUHDWDNXCLOHDPVAIFYDTEOJCHJMFFBYBQICVVKCFBQZTCRCDMDLPWOJNYP COZSCAPIZTHRAONKKSINEYBBWDVGRURGHBALLNKTXIGFWNKLQZPCTSMBRQYVMGXEIBGKILOUERUQSZIKLJQNKDPZJVSDIANCPNMTCRACOINNDA MOQOPAIVLAVJQWKZFANIEXSROWVPTCRRWMWEOIFZXRTNMYBGRZIKPJCTJYJQFKGVOKPTJYXUDCYYOIPMURGGXZGVLUDYKKODERMFIEIWKVSJAR DMDMBGKRQHSUCNHMIFNOOKAZIJQSDSIGSBRMCBLXMKFSZZUAJROFXWXYRGSBMDTXFEMBZEMCYBLNRDJBWBOCUMLSOLNUPTETGCYW ROACYQSFXBWNHGWPJVQNWAWKUVISCLHXAODXHGTGYBIVDGQQULRMEJMCYHRYXYWXLQTNEIINUCYEPKOEPHTQOQWVAZSBUDRHGYAF VQYNMYCERIVKOVOQNJLBIXTRBDBHNTZPWPYCVFUNIEAVJGCCWWHQQNTFCFYJDTKIZERPJVHSNNBWBOTMBMGRTKDWRLWPSEQAWSWD OFSPSEHOQRGFTQGBAGLJEZFNAHFMRNONCLEXLHXV

C:\Users\user\AppData\Local\Temp\tmpC5A6.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697358951122591
Encrypted:	false
SSDEEP:	24:GllFjmGrUw8wsY1UbsUhBRShwdYjDuvHNeGXNei:WFewtsZZp8DkHzNL
MD5:	244A1B624BD2C9C3A0D660425CB1F3C6
SHA1:	FB6C19991CC49A27F0277F54D88B4522F479BE5F
SHA-256:	E8C5EAACF4D2C4A65761719C311785A7873F0B25D849418ED86BBFE9D7F55C96
SHA-512:	9875E6DE2ACC859CACC2873F537DDE6ED4EC8CA00CBA3D28535E0440D76FFD475B66C52B6217D311D301C4B9A097619CF29A26B2FD54D03CD27A20A17EC9C 31
Malicious:	false
Preview:	GRXZDKKVDBUGJWVAVQNLKHTVWJFMWUAIFGXJYDZTDDYOZYAHDDDHNXHNVSFVZJEMKSJXGDABHWXKQZCQXBMLFZCFZRGZPZWYYNETLMDWOLDLPI FOVKRDMQEWUEHKITHNGNRTRZWQHFMBDECTTQKFDEVNVHBAPCNMCJNWWITPVACWBIUNPCYFZKGJXCMBWDNHDCVDCGEKHYPPPEGKPC PMYZEKRCOGRHDFANVZFDZEKZWOKLRIOUPCTJCKQPECVEEGNTLJWZOKHSKZRNLJEDQLEQNRWIYLSXHSNVGFTCDJOFJSSGANZFCFSTDUPYBCCAPQ WVVVHWQMAMBVDQNABQSQOSDYDMOVPXENCAXSTPDCENIQOWPCOQHPSISEOWFKMBLGAZRALPTAYHDZLKJTCHXGTPXNIVUMCOJRZXPU VUFPCWEAEZMMLATLTGHPJIMHWFBUWIATNBBPFGVFXNULJLRYLAGRNCKVAJADSLQGVLGIYOHDIWUERAQSCTFBMXCMLCXSHZGTWPBCVHUYPVAFSB ZNBGAGMHGULJYULEEHPGNBGEQRAOPBXXMZIUIPJMFAOVNMZZTOZGOZOJPKWCEFTTAVUBAADATZYJDWSZEZPLDTGYCYWTSDQTIMZHCKMQLZFEYS YUUWFJSYEFNDDKQMZVTBOZLQBDKFHMMKIYQPFKZLTSHIJVNPHPCTWBWPTTKDHDZEMDVWXXBLPWLCSSBMTLIVOVYOKQCJKTYJWGJUBQUGQVBYJQ QLLGTHWSPFLDMDWBTOQUISHXBCHIJKAJFIPBNKMWVQGUSJVNKXAXFDNOBYJXMWRDAZWUJSRMMFQXDPYYKOFBEROBQMDZHDZZHOEIOKDOCHQQDQ QRHOROOIFAGQEJZJFZIGPJIRWVNQYZAJAHAWIEFFNXLXQWIUWYSGZDFYPCCGWYBBFQQMSMJBRIUPFBWIHWJWVCYOBNNXKIIWTIXOWRVLFBGPGW FQTGPUNWKWUUMQXIKNCLTTGYHBMKXJ

C:\Users\user\AppData\Local\Temp\tmpC5A7.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696508269038202
Encrypted:	false
SSDEEP:	24:RSjVGe9uHEleifrd16Wa05tSl2jFQzpqPMXexMApqIjsp:2Ge9MQ/d16Wjtc2j64Phxjpq82
MD5:	0E9E92228B27AD7E7B4449467A529B0C
SHA1:	209F92CDFC879EE2B98DEF315CCE166AFEC00331
SHA-256:	284937D0EBFEDD95B2347297D957320D8D5CA5FC48218296767069CABA6B14A6
SHA-512:	CECA5F634268817B4A076414FFAB7D81F93EEC7E7D08B8691CCE0B2BCAF8FC6943654558 86E36983B4D8D758BC65BC1868BE8DB51AD41E082473726BB1FFD7 8
Malicious:	false
Preview:	PALRGUCVEHIRKBYGKJJWKNMNYKFUTLHCEDOTKTWJCZHNZMOUNMNREQTGFDNZTATQQPDFONRIRAZYJEPXQVIVWNBDQIMKULZMUINYTVUPNMQBQQ YLGCAJYFEIWZTWGYTHEJPFBRNGCTANCYOISUQMRINVDUEIROITGPJZCCOVCZIZBHLYBDARSNRLEOQQDWOSMHXNRNBXNWMRVAQZUASARYHEITVT VSLHRGBYURPTEUNAUCYMZTXOZXKDXUEUUVTNGWGSBRAWIJZDVZDLMZBKEVESROLUEDPITQGUXFSRFAVNSESAFZLNXMXUYRFUEUKCMNFITMUQEW TCKEGDPOXHJSXBDLFIOLLHDYIVOQVEYJEZMDIOFXZFCPXJEQLPCSHKUGRQKXAUMKTHUMHWFQZRGBRZHGHYRXRODJXEBANQHOOVFBZXKJHDCAAK HZGSWGKGEDWOOCFCEYHPAQBYBKRXOTJWSCPMRDXNRYAQFQHSHOFCHWJDKTFHACROGLPZFWDCIBJSUTMTRHJKEGAHSBAQLDTWPTXB LVYYBNJBKDUNGOUDVWZOBKOJKSMZERYOYBNMDSYUPHFDPUXOMKCYNSEBJHJVXSWTIMBDLPWYMYMQKYICPQEWMYDUMYJRSVQHDEELUFOEQYUIZB TNUNJNZQTDTIJKNOJNFJDDGEYVGDXTQINCQDGJRRPOBRUHQLMKFJSSNNCQMDHWQYMHWIBVNPHRQCBTMYBSOJYXCUAYTWUDETCJTTEQSPXKTRSQ BDJYENXLXJTQIYOZHEFAQOFBXKATTASAWEYGDPTTLZDAFVKRYLRNFSWZYBGUMRHHMNPVCVECBEVWEXNMSCXSGJRAQKAYEIULWHXXFKTJWPDMYU AOSFBKCTNCTQQXTLXIIJKYOPYBMSFGYLZDGOXTVIHYLUMJCRDRQXFLBDAUXBTNAPMACHVQILKZSQLNPPJVGXAXUMTOUMJJJYJSPJALITYYHOOM VVOQNOSSPBLMRBWWPYXB

C:\Users\user\AppData\Local\Temp\tmpC810.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728

C:\Users\user\AppData\Local\Temp\tmpC810.tmp	
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\tmpC811.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmpC841.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.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\tmpC842.tmp	
Process:	C:\Users\user\Desktop\6UclBifP3f.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpC842.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.517924395726936
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:	6UclBifP3f.exe
File size:	370176
MD5:	1adb2662c75187ef4aad7be7f16a8f4d
SHA1:	50334d8144ca8278f83ca279d22d142637acd341
SHA256:	e620189fa4c882f2ec63faed4c07b2a924b7231403513791ce761f7d814ee2c0
SHA512:	53f1af03fb85fc02679a28ed07ccd548601d5eeb89bc28b76ea4aea3062b55a78fea6b17358b9005ca9cae67aa51b0bfdcf5ea263baac30776bf76f38d91cdda
SSDEEP:	6144:nIr2R1bj/slGbEK4714ynsu/Nep/t75JoKJdjWWEb8ri7y5U:nIr2Pj/sl9nxNItTJNwbboU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".f.y.f.y.f.y.....M.y.....v.y.....y.o...e.y.f.x...y.....g.y.....g.y.....g.y.Richf.y.....PE..L...W=s_.....

File Icon

Icon Hash:	aedaae9ec6a68aa4

Static PE Info

General

Entrypoint:	0x401c60
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F733D57 [Tue Sep 29 13:57:43 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	9680696139920742654 63fec272c56c9

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1910b	0x19200	False	0.454912935323	data	6.23838899825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x8596	0x8600	False	0.285535214552	data	4.59585890512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x24000	0x2768924	0x23800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x278d000	0x4770	0x4800	False	0.730631510417	data	6.48326135377	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2792000	0x1098c	0x10a00	False	0.077537593985	data	1.00022544426	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:06:42.996685028 CEST	192.168.2.3	8.8.8.8	0x2984	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:06:43.035728931 CEST	192.168.2.3	8.8.8.8	0xb7ef	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 10:06:43.019372940 CEST	8.8.8.8	192.168.2.3	0x2984	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:06:43.055876970 CEST	8.8.8.8	192.168.2.3	0xb7ef	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: 6UclBifP3f.exe PID: 3372 Parent PID: 5472

General

Start time:	10:06:11
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\6UclBifP3f.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6UclBifP3f.exe'
Imagebase:	0x400000
File size:	370176 bytes
MD5 hash:	1ADB2662C75187EF4AAD7BE7F16A8F4D
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: 00000000.00000002.402230300.0000000005E15000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.396975534.0000000004DE0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.395986015.00000000048C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.315015554.0000000002E8B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.396296874.00000000049AC000.00000004.00000001.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: 2248 Parent PID: 3372

General

Start time:	10:06:12
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis