ID: 490267
Sample Name:
JSHRF6iG8A.exe
Cookbook: default.jbs
Time: 10:25:41
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

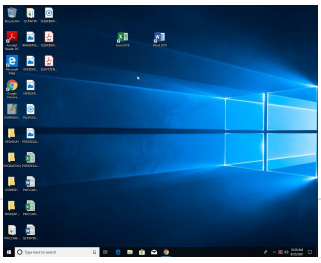
Windows Analysis Report JSHRF6iG8A.exe

Overview

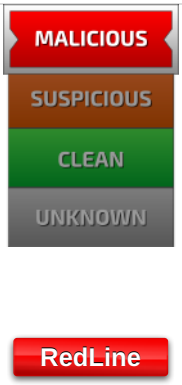
General Information

Sample Name:	JSHRF6iG8A.exe
Analysis ID:	490267
MD5:	bf15cb801b1919a.
SHA1:	544aa302f49a250.
SHA256:	ab3288194f8b541.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

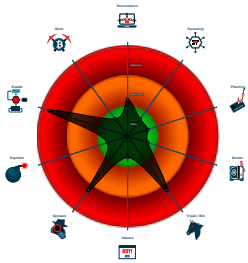


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Wallets
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- Tries to harvest and steal browser in…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- JSHRF6iG8A.exe (PID: 4036 cmdline: 'C:\Users\user\Desktop\JSHRF6iG8A.exe' MD5: BF15CB801B1919A71B0979EFA22F4B52)
  - conhost.exe (PID: 6284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.372796000.00000000061E5000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.370613149.0000000004E00000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.369773109.0000000004A30000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.291845822.0000000002D9B000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.370541857.0000000004C0C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.JSHRF6iG8A.exe.4c4c98e.5.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.JSHRF6iG8A.exe.2d9b618.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.JSHRF6iG8A.exe.4a30000.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.JSHRF6iG8A.exe.4e00000.6.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.JSHRF6iG8A.exe.4a30ee8.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

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

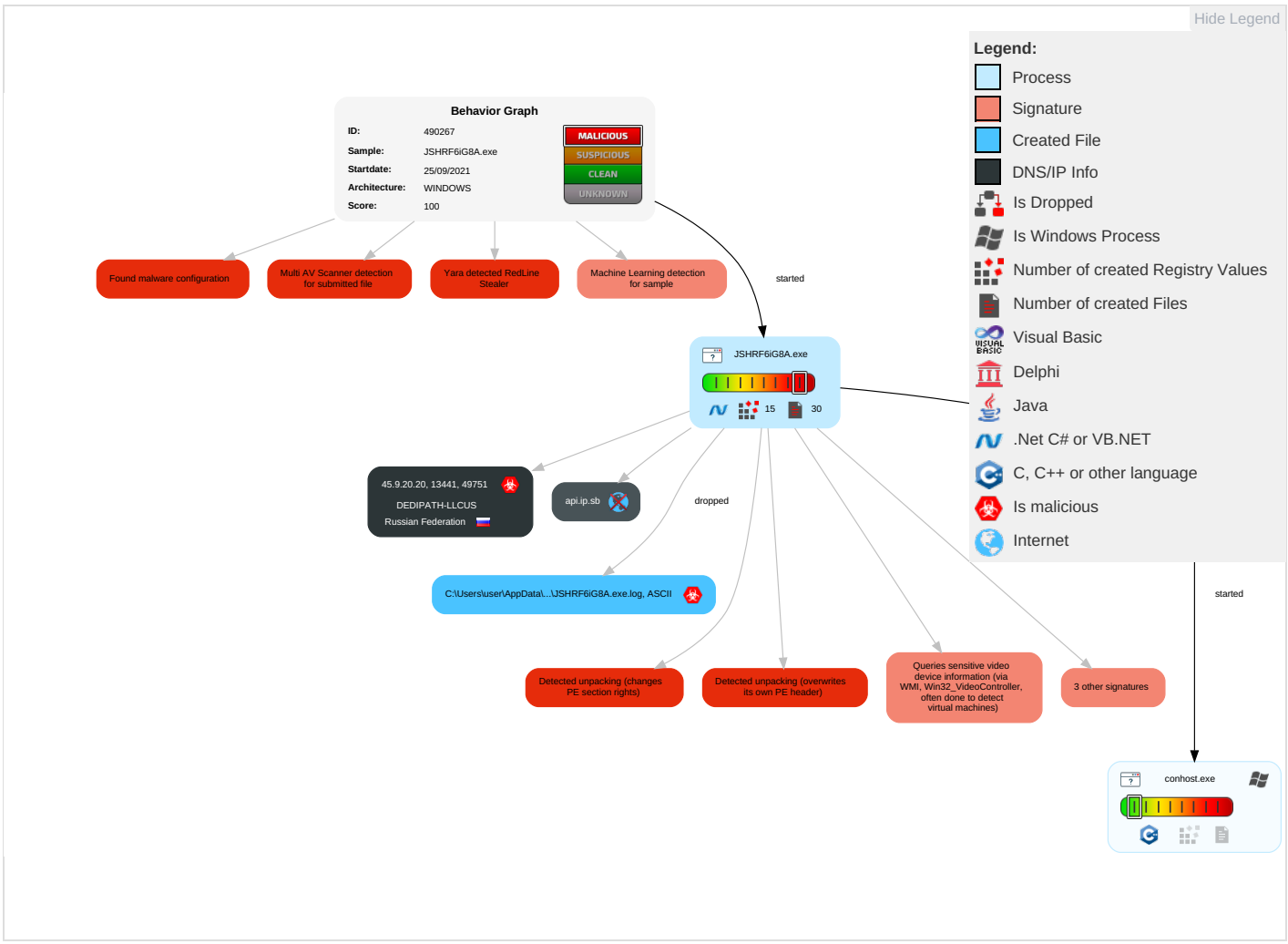
Remote Access Functionality:

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	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redire 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

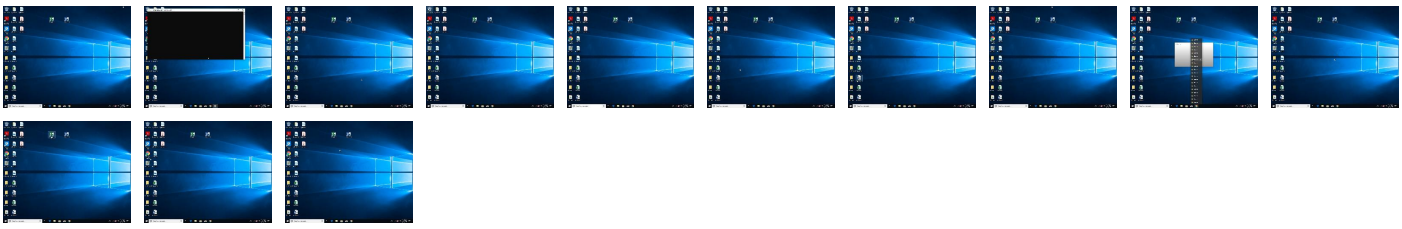
Behavior Graph



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
JSHRF6iG8A.exe	32%	Virustotal		Browse
JSHRF6iG8A.exe	50%	ReversingLabs	Win32.Trojan.Glupteba	
JSHRF6iG8A.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/PartDiscord	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://https://www.bing.W	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://https://search.yaho	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	

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:	490267
Start date:	25.09.2021
Start time:	10:25:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JSHRF6iG8A.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@2/25@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.9% (good quality ratio 18.2%) • Quality average: 84.6% • Quality standard deviation: 23.6%
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
10:27:05	API Interceptor	63x Sleep call for process: JSHRF6iG8A.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.9.20.20	nonLjpZDon.exe	Get hash	malicious	Browse	
	RzDaHvcf7g.exe	Get hash	malicious	Browse	
	Z5kAk5QCIB.exe	Get hash	malicious	Browse	
	QH3hnrCD8x.exe	Get hash	malicious	Browse	
	5DxtZ6xMrB.exe	Get hash	malicious	Browse	
	qefGuXETjf.exe	Get hash	malicious	Browse	
	aVfFzvm8iR.exe	Get hash	malicious	Browse	
	6UclBifP3f.exe	Get hash	malicious	Browse	
	jroJZULz8w.exe	Get hash	malicious	Browse	
	976y4GH2rY.exe	Get hash	malicious	Browse	
	3zb0mumThM.exe	Get hash	malicious	Browse	
	Z1LjJ5odpI.exe	Get hash	malicious	Browse	
	JGam14245S.exe	Get hash	malicious	Browse	
	rj6qxIrooh.exe	Get hash	malicious	Browse	
	EZpSqv83eJ.exe	Get hash	malicious	Browse	
	SCym9cuPKq.exe	Get hash	malicious	Browse	
	yqxz73qFDp.exe	Get hash	malicious	Browse	
	W6fjwqXDfO.exe	Get hash	malicious	Browse	
	NcX0SHPIGm.exe	Get hash	malicious	Browse	
	eucPRBGIG4.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	nonLjpZDon.exe	Get hash	malicious	Browse	• 45.9.20.20
	RzDaHvcf7g.exe	Get hash	malicious	Browse	• 45.9.20.20
	Z5kAk5QCIB.exe	Get hash	malicious	Browse	• 45.9.20.20
	QH3hnrCD8x.exe	Get hash	malicious	Browse	• 45.9.20.20
	5DxtZ6xMrB.exe	Get hash	malicious	Browse	• 45.9.20.20
	qefGuXETjf.exe	Get hash	malicious	Browse	• 45.9.20.20
	aVfFzvm8iR.exe	Get hash	malicious	Browse	• 45.9.20.20
	6UclBifP3f.exe	Get hash	malicious	Browse	• 45.9.20.20
	jroJZULz8w.exe	Get hash	malicious	Browse	• 45.9.20.20
	976y4GH2rY.exe	Get hash	malicious	Browse	• 45.9.20.20
	3zb0mumThM.exe	Get hash	malicious	Browse	• 45.9.20.20
	Z1LjJ5odpI.exe	Get hash	malicious	Browse	• 45.9.20.20
	JGam14245S.exe	Get hash	malicious	Browse	• 45.9.20.20
	rj6qxIrooh.exe	Get hash	malicious	Browse	• 45.9.20.20
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 45.133.1.182
	EZpSqv83eJ.exe	Get hash	malicious	Browse	• 45.9.20.20
	SCym9cuPKq.exe	Get hash	malicious	Browse	• 45.9.20.20
	yqxz73qFDp.exe	Get hash	malicious	Browse	• 45.9.20.20
	W6fjwqXDfO.exe	Get hash	malicious	Browse	• 45.9.20.20
	NcX0SHPIGm.exe	Get hash	malicious	Browse	• 45.9.20.20

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JSHRF6iG8A.exe.log	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp1E0.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp1E0.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\tmp1E1.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp1E2.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp1E3.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp213.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp214.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp282.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp28F7.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp28F7.tmp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp28F8.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp28F9.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp28FA.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp28FB.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp292B.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp292C.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp2A85.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp2A85.tmp	
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A86.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp755B.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmp755C.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmpDA9F.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmpDAA0.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.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\tmpE24.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6969712158039245
Encrypted:	false
SSDEEP:	24:zDLHcjI8IQ6sNUYzo1jfRRMF6zzC3ZzNTWx7M00:zDL4ImUYzebRR66C3Z0JMR
MD5:	31CD00400A977C512B9F1AF51F2A5F90
SHA1:	3A6B9ED88BD73091D5685A51CB4C8870315C4A81
SHA-256:	E01ADE9C56AF2361A5ADC05ADE2F5727DF1B80311A0FDC6F15B2E0FFFACC9067
SHA-512:	0521ED245FA8F46DE9502CD53F5A50B01B4E83983CC6D9DE0CF02E54D2825C1C26A748CC27E24633DA1171CE0309323235ECF7EB536D4058214D7618794CF2F
Malicious:	false
Preview:	PWCCAWLGRESZQJYMKOMIHTZVFVPFCSAZVTKGMPWIGSDMTLFZQLHJERDPYZCJGFCRLISWNBAMIMDXCWDVGVLWLRBEVYOOPHYWACKPZXSURGSIFW TFUJKLSAQNAJEWDLUIKFHXLUAMUDGRAVFMICAHEZBIIEGWGAVVJHMHSIBGNLEHYVSOKQMYABDYCPEBOGBMYUCIGVRGYYQRAYNYHAIBMHOTRIZL LYBECMXTCFUOVXXHSEMIUWSBDHOZIZZUXFTLKXXNEMXBKLCQDPKVZNOMDYUYJRWCVILZVJDNNBMPTNOFSKRQTILJRXTKDNUIYSQCAOPCQKTXYX PPGZDZOQYLGYFPFIWNBSQZXYABPTNBJQNBZEETJSFXZNHXBRWUHOMCZAGZQJLNPMZFALBBPHBIXZHLBTBJLTUHPUYVUDWDFJANSIIDJVMUYLPZ PYGAJWMTOHGILQWHKJDQUWMTSWIBVVZGAHCNWIFZNGNERRKMSIVXWXEXRZZEWYASCIYJYCOOBWRTNZELPWKFVZKZIBGQBLGCTSTNAJSWPHYJCQ SYZVFRYFSRAVVXJIOHQCNVEOIMWPEAVCJLBHRUKDHJWPFMXAKTZVQCOUKYCBZFWBREKKHOHZVNMMJZGWIZEYRAIKTHMJRCWVWKNMJNSZHSDRUZ SQOJKCTOSNGKOKEAWUIQNIYHWKIIDHKQIJWCSGRRLEVUTENXSNNVDVYDJTIWYNCAZIEBXMIROLIBTLMGEUOCECFFWLENTJSVHFKQHKAPBXQAJJ SUOUSFCBQTHCFYZGSVVAUPLQELRWLXRCZSUSFUBCORCWMJPUNHTEEYODSFGJFTDZLLXMQYMIHIZXOYGABIAWYSBWLAJSCKBWGJBVMMJKBKLUHU LJIUHQXIXESAUTNVVZNKMIVIOHPPQAWTQSEHTQMIWNPRZRETXZHRGWOTGIEHCCSGIUCKCIFCQPTAJOFCIMYSMCOPGASEEYCNQLXCNRAPQUSQXT WPKPYCQXPE

C:\Users\user\AppData\Local\Temp\tmpE25.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702247102869977
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmpE25.tmp	
SSDEEP:	24:GwASqxXUeo2spEcwb4NnVEBb2Ag1EY9TDqVEQXZvnIx+:nAD1U6+Lwb4dV42x1EIeVlXZ/5
MD5:	B734D7226D90E4FD8228EE89C7DD26DA
SHA1:	EDA7F371036A56A0DE687FF97B01F355C5060846
SHA-256:	ED3AE18072D12A2B031864F502B3DA672B4D4FA8743BEC8ADE114460F53C24D6
SHA-512:	D11ED908D0473A6BEA78D56D0E46FC05DAE642C6ED2F6D60F7859BB25C596CDAA79CC7883FEA5C175A2C04BD176943FF45670B19D6A55B3D5F29FAF40A19A 20
Malicious:	false
Preview:	QCFWYSKMHARLAFTMDAYCDPDNVLLXYAHYJQVDDKWMWZXTODMVQHOWYAKZGPKJEHLDEADLWAOYFHCRBONQYOLNJKXLXXPSVNNBUMGS SHSRYIKKLNWBJSSZQFZBFWIPYYALBWYXPUCHCBPPPRVICZHAAXDBSBDAFSJSLRPZCKMILDLKTZJTTJWTRDUXPIOSWYRPJKVLJAGHSGEPPERRAQ LAJLIRGZPORRNBHIKYMYWHJJKNXIQOPDJPXFLFPWXDCSZYFDTACTIFVHTTSPLEYMJQGMJBZKBTPKCSRPHSAJZDKKKDYFDICXMYAQSFGBCKRXTF XXUYCXPOOHXIGGOZQXUOJXGUHUEOJLEOQQRFQRNQSWAOWAWOUVFMKBPTZVBCGRCYEHPXUWCDBHICKJYVGTNPPMEWNTSWYZNREIVB OXSICNBJXTOOMRYUPEHBVWMTIZHWLGFFTIUYFBQKZOWLOZMSGJFBUHXKMGISFGKCABOUUUQJAUODQPPYPQJGLZVADLCCGHPBEUWSDDXYCCQVTR QWCEJDTNAGHKGJTRWVAQBQJBUQWMJRXXASIQFFIUCPKMEXTJTVBDCBEYZDLKHCHQXMUBNRVRITBTYGULZYWAXVJAXNQEPONBFIAUWZCXQYHHPH ZWKKUTNXAQELCSUFKXKKQLLKNVNOREOWTEVCFHSUGPNRMAPAFPTHPGPAJPOCFBZXTIYQYUSEJFOUEZDUJSRXDHTOZAMMNCCIXWLXFQZALVARMP TDBNFJAJUMFQAHUJVWMEIDRIMZQXYHMCNBVLONHTHCXFAKSQBBXFBBFYSTIWNRKGOIHMIHZKIQSYCSFIRGLYFATERWSKAZLTFNMKHFVBLMXNER MNYZHBEYHNFPIPCGHZZMBNNYITUETKSXMZHNSGROLAGIITATFDCBZCBLYQHHYFPBDWGCTQNYPHDHFBNVEJJDIVMSPKDXKQBUNSMLJDVGOKQUEV KEVEUUSGEQJDKGYLPIDXNBIPBAJRUU

C:\Users\user\AppData\Local\Temp\tmpE26.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6969712158039245
Encrypted:	false
SSDEEP:	24:zDLHcjl8IQ6sNUYzo1jfRRMF6zzC3ZzNTWx7M00:zDL4ImUYzebRR66C3Z0JMR
MD5:	31CD00400A977C512B9F1AF51F2A5F90
SHA1:	3A6B9ED88BD73091D5685A51CB4C8870315C4A81
SHA-256:	E01ADE9C56AF2361A5ADC05ADE2F5727DF1B80311A0FDC6F15B2E0FFFACC9067
SHA-512:	0521ED245FA8F46DE9502CD53F5A50B01B4E83983CC6D9DE0CF02E54D2825C1C26A748CC27E24633DA1171CE0309323235ECF7EB536D4058214D7618794CF2F
Malicious:	false
Preview:	PWCCAWLGRESZQJYMKOMIHTZVFVPFCSAZVTKGMPWIGSDMTLFZQLHJERDPYZCJGFCRLISWNBAMIMDXCWDVGVLWLRBEVYOOPHYWACKPZXSURGSIFW TFUJKLSAQNAJEWDLUIKFHXLUAMUDGRAVFMICAHEZBIIEGWGAVVJHMHSIBGNLEHYVSOKQMYABDYCPEBOGBMYUCIGVRGYYQRAYNYHAIBMHOTRIZL LYBECMXTCFUOVXXHSEMIUWSBDHOZIZZUXFTLKXXNEMXBKLCQDPKVZNOMDYUYJRWCVILZVJDNNBMPTNOFSKRQTILJRXTKDNUIYSQCAOPCQKTXYX PPGZDZOQYLGYFPFIWNBSQZXYABPTNBJQNBZEETJSFXZNHXBRWUHOMCZAGZQJLNPMZFALBBPHBIXZHLBTBJLTUHPUYVUDWDFJANSIIDJVMUYLPZ PYGAJWMTOHGILQWHKJDQUWMTSWIBVVZGAHCNWIFZNGNERRKMSIVXWXEXRZZEWYASCIYJYCOOBWRTNZELPWKFVZKZIBGQBLGCTSTNAJSWPHYJCQ SYZVFRYFSRAVVXJIOHQCNVEOIMWPEAVCJLBHRUKDHJWPFMXAKTZVQCOUKYCBZFWBREKKHOHZVNMMJZGWIZEYRAIKTHMJRCWVWKNMJNSZHSDRUZ SQOJKCTOSNGKOKEAWUIQNIYHWKIIDHKQIJWCSGRRLEVUTENXSNNVDVYDJTIWYNCAZIEBXMIROLIBTLMGEUOCECFFWLENTJSVHFKQHKAPBXQAJJ SUOUSFCBQTHCFYZGSVVAUPLQELRWLXRCZSUSFUBCORCWMJPUNHTEEYODSFGJFTDZLLXMQYMIHIZXOYGABIAWYSBWLAJSCKBWGJBVMMJKBKLUHU LJIUHQXIXESAUTNVVZNKMIVIOHPPQAWTQSEHTQMIWNPRZRETXZHRGWOTGIEHCCSGIUCKCIFCQPTAJOFCIMYSMCOPGASEEYCNQLXCNRAPQUSQXT WPKPYCQXPE

C:\Users\user\AppData\Local\Temp\tmpE27.tmp	
Process:	C:\Users\user\Desktop\JSHRF6iG8A.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702247102869977
Encrypted:	false
SSDEEP:	24:GwASqxXUeo2spEcwb4NnVEBb2Ag1EY9TDqVEQXZvnIx+:nAD1U6+Lwb4dV42x1EIeVlXZ/5
MD5:	B734D7226D90E4FD8228EE89C7DD26DA
SHA1:	EDA7F371036A56A0DE687FF97B01F355C5060846
SHA-256:	ED3AE18072D12A2B031864F502B3DA672B4D4FA8743BEC8ADE114460F53C24D6
SHA-512:	D11ED908D0473A6BEA78D56D0E46FC05DAE642C6ED2F6D60F7859BB25C596CDAA79CC7883FEA5C175A2C04BD176943FF45670B19D6A55B3D5F29FAF40A19A 20
Malicious:	false
Preview:	QCFWYSKMHARLAFTMDAYCDPDNVLLXYAHYJQVDDKWMWZXTODMVQHOWYAKZGPKJEHLDEADLWAOYFHCRBONQYOLNJKXLXXPSVNNBUMGS SHSRYIKKLNWBJSSZQFZBFWIPYYALBWYXPUCHCBPPPRVICZHAAXDBSBDAFSJSLRPZCKMILDLKTZJTTJWTRDUXPIOSWYRPJKVLJAGHSGEPPERRAQ LAJLIRGZPORRNBHIKYMYWHJJKNXIQOPDJPXFLFPWXDCSZYFDTACTIFVHTTSPLEYMJQGMJBZKBTPKCSRPHSAJZDKKKDYFDICXMYAQSFGBCKRXTF XXUYCXPOOHXIGGOZQXUOJXGUHUEOJLEOQQRFQRNQSWAOWAWOUVFMKBPTZVBCGRCYEHPXUWCDBHICKJYVGTNPPMEWNTSWYZNREIVB OXSICNBJXTOOMRYUPEHBVWMTIZHWLGFFTIUYFBQKZOWLOZMSGJFBUHXKMGISFGKCABOUUUQJAUODQPPYPQJGLZVADLCCGHPBEUWSDDXYCCQVTR QWCEJDTNAGHKGJTRWVAQBQJBUQWMJRXXASIQFFIUCPKMEXTJTVBDCBEYZDLKHCHQXMUBNRVRITBTYGULZYWAXVJAXNQEPONBFIAUWZCXQYHHPH ZWKKUTNXAQELCSUFKXKKQLLKNVNOREOWTEVCFHSUGPNRMAPAFPTHPGPAJPOCFBZXTIYQYUSEJFOUEZDUJSRXDHTOZAMMNCCIXWLXFQZALVARMP TDBNFJAJUMFQAHUJVWMEIDRIMZQXYHMCNBVLONHTHCXFAKSQBBXFBBFYSTIWNRKGOIHMIHZKIQSYCSFIRGLYFATERWSKAZLTFNMKHFVBLMXNER MNYZHBEYHNFPIPCGHZZMBNNYITUETKSXMZHNSGROLAGIITATFDCBZCBLYQHHYFPBDWGCTQNYPHDHFBNVEJJDIVMSPKDXKQBUNSMLJDVGOKQUEV KEVEUUSGEQJDKGYLPIDXNBIPBAJRUU

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.518763941702596
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:	JSHRF6iG8A.exe
File size:	370176
MD5:	bf15cb801b1919a71b0979efa22f4b52
SHA1:	544aa302f49a2509cd5faf42c424d38a03545fcb
SHA256:	ab3288194f8b5415adfd976b30e88cf5baacb4492c55420799dca60475a76933
SHA512:	52c446ed79ba77cfcc09c57a04d41b9312537422925346a72ad7b59b042824fa32697040b254cefe8a1b2721ebc279ae2f51e7d1e6571007e1c13a895d0d8962
SSDEEP:	6144:hor9uc9j0glebPPyN0Kf4ZEWLJR/wlxOzdS1:hor9Tj0glcPzlEWdBQxOzdS1
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...x@.^.....

File Icon

Icon Hash:	aadaae9ec6a68aa4

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:	0x5EAD4078 [Sat May 2 09:42:16 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	0.454903218284	data	6.23513152914	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x8596	0x8600	False	0.285360307836	data	4.59525013686	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x24000	0x2768984	0x23800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x278d000	0x4770	0x4800	False	0.730523003472	data	6.48164125224	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2792000	0x10974	0x10a00	False	0.0774788533835	data	0.999639477206	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 10:27:05.603504896 CEST	192.168.2.3	8.8.8.8	0x438	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:27:05.634268999 CEST	192.168.2.3	8.8.8.8	0x77f3	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 10:27:05.623111010 CEST	8.8.8.8	192.168.2.3	0x438	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:27:05.657361031 CEST	8.8.8.8	192.168.2.3	0x77f3	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: JSHRF6iG8A.exe PID: 4036 Parent PID: 4780

General

Start time:	10:26:36
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\JSHRF6iG8A.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JSHRF6iG8A.exe'
Imagebase:	0x400000
File size:	370176 bytes
MD5 hash:	BF15CB801B1919A71B0979EFA22F4B52
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: 00000000.00000002.372796000.00000000061E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.370613149.0000000004E00000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.369773109.0000000004A30000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.291845822.0000000002D9B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.370541857.0000000004C0C000.00000004.00000001.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: 6284 Parent PID: 4036

General

Start time:	10:26:37
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