ID: 458956
Sample Name:
7d9bXpW0im.exe
Cookbook: default.jbs
Time: 22:47:17
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

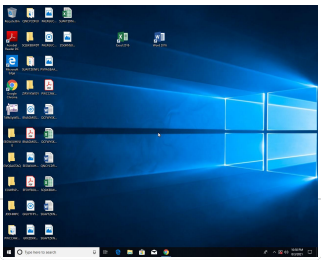
Windows Analysis Report 7d9bXpW0im.exe

Overview

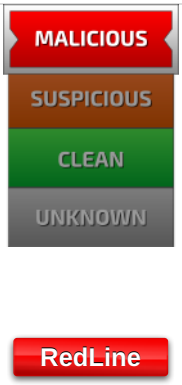
General Information

Sample Name:	7d9bXpW0im.exe
Analysis ID:	458956
MD5:	0f838cf9ac70e70..
SHA1:	01ab9926ff27f0d…
SHA256:	b1445b8206b5f2f..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

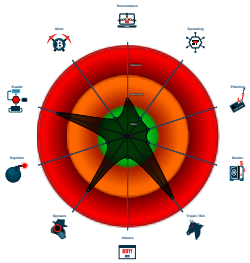


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Multi AV Scanner detection for subm…
- Yara detected RedLine Stealer
- Yara detected RedLine Stealer
- Machine Learning detection for samp…
- PE file contains section with special…
- PE file has nameless sections
- Performs DNS queries to domains w…
- Queries sensitive disk information (v…
- Queries sensitive video device inform…
- Tries to harvest and steal browser in…
- Tries to steal Crypto Currency Wallets

Classification



Process Tree

- **System is w10x64**
- 7d9bXpW0im.exe (PID: 3440 cmdline: 'C:\Users\user\Desktop\7d9bXpW0im.exe' MD5: 0F838CF9AC70E706AB24F4555618186C)
  - conhost.exe (PID: 4564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.261102430.0000000009D70000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 7d9bXpW0im.exe PID: 3440	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 7d9bXpW0im.exe PID: 3440	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.7d9bXpW0im.exe.9d70000.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Performs DNS queries to domains with low reputation

System Summary:

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected RedLine Stealer

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality:

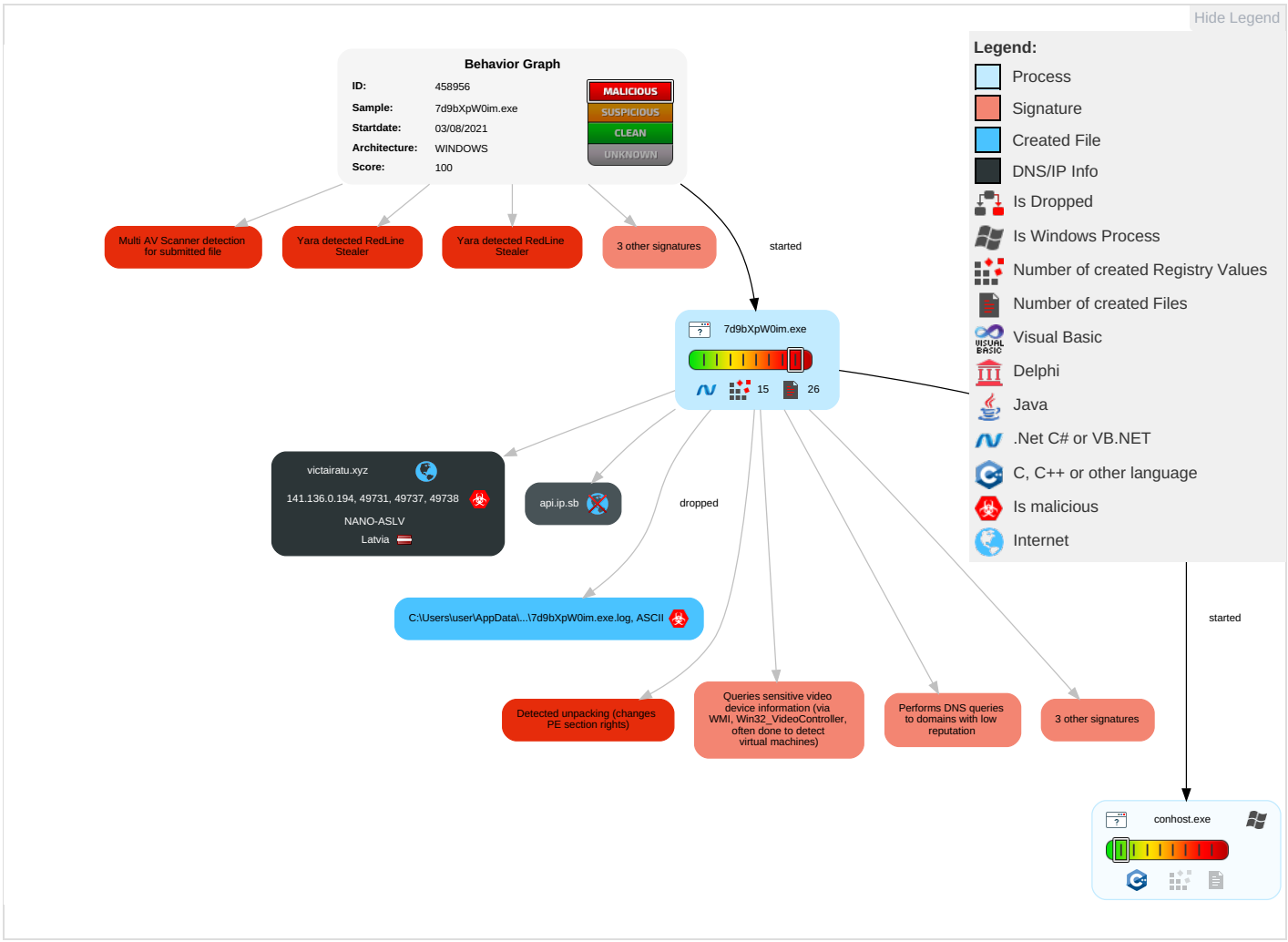
Yara detected RedLine Stealer

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	Security Software Discovery 2 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comn
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Explo Redir Calls/
Domain Accounts	At (Linux)	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	Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	System Information Discovery 1 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic

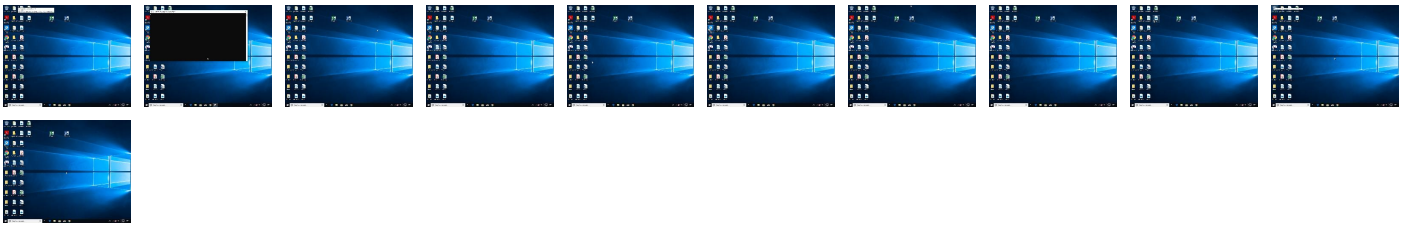
Behavior Graph



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
7d9bXpW0im.exe	30%	Virustotal		Browse
7d9bXpW0im.exe	31%	Metadefender		Browse
7d9bXpW0im.exe	54%	ReversingLabs	ByteCode-MSIL.Packed.Confuser	
7d9bXpW0im.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.7d9bXpW0im.exe.90000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
victairatu.xyz	1%	Virustotal		Browse
api.ip.sb	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://victairatu.xyz4	0%	Avira URL Cloud	safe	
http://victairatu.xyz	1%	Virustotal		Browse
http://victairatu.xyz	0%	Avira URL Cloud	safe	
http://victairatu.xyz4/l	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettings	0%	Avira URL Cloud	safe	
http://tempuri.org/t_	0%	Avira URL Cloud	safe	
http://victairatu.xyz:80/	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://victairatu.xyz/	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	Avira URL Cloud	safe	
http://go.micros	0%	URL Reputation	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/GetUpdates	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnectResponse	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://helpx.ad	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnect	0%	Avira URL Cloud	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://https://api.ip.sb4/l	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
victairatu.xyz	141.136.0.194	true	true	• 1%, Virustotal, Browse	unknown
api.ip.sb	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://victairatu.xyz/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
141.136.0.194	victairatu.xyz	Latvia		43513	NANO-ASLV	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458956
Start date:	03.08.2021
Start time:	22:47:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7d9bXpW0im.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:	21
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@2/21@5/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.5%) • Quality average: 38.9% • Quality standard deviation: 38.6%
HCA Information:	• Successful, ratio: 92% • 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
22:48:22	API Interceptor	69x Sleep call for process: 7d9bXpW0im.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
141.136.0.194	JY2WV2vcxy.exe	Get hash	malicious	Browse	• readingli stforjuly9.xyz/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kLRJewibGm.exe	Get hash	malicious	Browse	• readingli stforjuly9.xyz/
	WWzUml7m53.exe	Get hash	malicious	Browse	• readingli stforjuly9.xyz/
	e7V79qGVJT.exe	Get hash	malicious	Browse	• readingli stforjuly9.xyz/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NANO-ASLV	SecuriteInfo.com.W32.AIDetect.malware1.4421.exe	Get hash	malicious	Browse	• 141.136.0.194
	NKqz6BNPdi.exe	Get hash	malicious	Browse	• 141.136.0.194
	JY2WV2vcxy.exe	Get hash	malicious	Browse	• 141.136.0.194
	kLRJewibGm.exe	Get hash	malicious	Browse	• 141.136.0.194
	4kWyL2w4wQ	Get hash	malicious	Browse	• 185.71.138.18
	64AF392E3667F1261AEB70AE530C4E47AF1BA01834B3C.exe	Get hash	malicious	Browse	• 141.136.0.113
	Dpjv8G9gX5.exe	Get hash	malicious	Browse	• 141.136.0.194
	WWzUml7m53.exe	Get hash	malicious	Browse	• 141.136.0.194
	e7V79qGVJT.exe	Get hash	malicious	Browse	• 141.136.0.194
	IsVEKYHPfW.exe	Get hash	malicious	Browse	• 141.136.0.74
	e0gtwzAmth.exe	Get hash	malicious	Browse	• 141.136.0.181
	R9SMlzY1qf.exe	Get hash	malicious	Browse	• 141.136.0.181
	5F8i5lJ4oT.exe	Get hash	malicious	Browse	• 141.136.0.181
	nJmAgu7z7p.exe	Get hash	malicious	Browse	• 141.136.0.181
	case_L0275390548.xlsb	Get hash	malicious	Browse	• 141.136.0.170
	case_L0275390548.xlsb	Get hash	malicious	Browse	• 141.136.0.170
	case_L0275390548.xlsb	Get hash	malicious	Browse	• 141.136.0.170
	WFtMGdZxjT.exe	Get hash	malicious	Browse	• 141.136.0.181
	seH7cBPXgW.exe	Get hash	malicious	Browse	• 141.136.0.181
	5dS4AGw2fG.exe	Get hash	malicious	Browse	• 141.136.0.181

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7d9bXpW0im.exe.log	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2502
Entropy (8bit):	5.3347050065951125
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKdHKBSTHaAHKzvRYHKhQnoPtHoxHImHKhBHKoHaHZHAHxLHG1qHjS:vq5qXAqdqslqzJYqhQnoPtlxHbqLqo6p
MD5:	2BF079EA03BF5AB82640736A9F171908
SHA1:	232A8C975E57B3124752F9A9A97D769E7EFF6027
SHA-256:	FC5BCB6E64913F48A49217B6625EE6942D3C7C166AC7AB1F699662E782982F12
SHA-512:	CF536D0F7BF5668E4CF2E03A08745E1EF3F6FC21573D2BE9B194F31BC64878FB60CA3DCDDD30D39D41A732FDB39CE0305EE9C3AAD33AC90712D6D9DBB392195
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7d9bXpW0im.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp2C93.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2C94.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2C95.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Temp\tmp2C95.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2C96.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2C97.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2CC7.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp2CC8.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe

C:\Users\user\AppData\Local\Temp\tmp2CC8.tmp	
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\tmp2CC9.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp2CF9.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp2CFA.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp2CFA.tmp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp3EB.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp3EC.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp5591.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmp5592.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\tmp5592.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\tmpB150.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmpB151.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmpDAD3.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpDAD3.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpDAD4.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmpDB04.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.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\tmpDB05.tmp	
Process:	C:\Users\user\Desktop\7d9bXpW0im.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.2958132242584455
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	7d9bXpW0im.exe
File size:	273408
MD5:	0f838cf9ac70e706ab24f4555618186c
SHA1:	01ab9926ff27f0d253d63fe34c743bbbab05ee8f
SHA256:	b1445b8206b5f2f15cd8d9a7bb8e0b551491ed72cb07ccb5f2a1f877b084396c
SHA512:	f5d8695d327a9e0221e42fb7041c3d325294d2aa1e13c086fe2137a5bd76a3cf8545191bfa60e13e8cc72d1d24d7236a80504ab48f5bff48de20752cc89348d4
SSDEEP:	6144:vp4qqCFPFGPwRI8g1LjsP/N3S/KT1/i+CKYun2f:sCyYtUL7s/W
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....n..... ....@.. .....@.....

File Icon

Icon Hash:	f6cc829adea656d6

Static PE Info

General

Entrypoint:	0x44a00a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6103CB83 [Fri Jul 30 09:50:59 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
vMF<;	0x2000	0x2a6c4	0x2a800	False	1.0003504136	data	7.99898892703	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x2e000	0x6a70	0x6c00	False	0.560040509259	data	6.09281772311	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x36000	0x10e50	0x11000	False	0.159380744485	data	3.8826680912	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x48000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x4a000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:48:14.098021984 CEST	192.168.2.3	8.8.8.8	0x8162	Standard query (0)	victairatu.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 22:48:22.104491949 CEST	192.168.2.3	8.8.8.8	0x5327	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Aug 3, 2021 22:48:22.152965069 CEST	192.168.2.3	8.8.8.8	0x12f8	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Aug 3, 2021 22:48:30.295046091 CEST	192.168.2.3	8.8.8.8	0xcf7e	Standard query (0)	victairatu.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 22:48:30.825989962 CEST	192.168.2.3	8.8.8.8	0x2f1d	Standard query (0)	victairatu.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:48:14.133831024 CEST	8.8.8.8	192.168.2.3	0x8162	No error (0)	victairatu.xyz		141.136.0.194	A (IP address)	IN (0x0001)
Aug 3, 2021 22:48:22.143460989 CEST	8.8.8.8	192.168.2.3	0x5327	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:48:22.186495066 CEST	8.8.8.8	192.168.2.3	0x12f8	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:48:30.327512026 CEST	8.8.8.8	192.168.2.3	0xcf7e	No error (0)	victairatu.xyz		141.136.0.194	A (IP address)	IN (0x0001)
Aug 3, 2021 22:48:30.868684053 CEST	8.8.8.8	192.168.2.3	0x2f1d	No error (0)	victairatu.xyz		141.136.0.194	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- victairatu.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49731	141.136.0.194	80	C:\Users\user\Desktop\7d9bXpW0im.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:48:14.348303080 CEST	1157	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/CheckConnect" Host: victairatu.xyz Content-Length: 137 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Aug 3, 2021 22:48:14.392528057 CEST	1157	IN	HTTP/1.1 100 Continue
Aug 3, 2021 22:48:14.509370089 CEST	1159	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 20:48:14 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 38 63 0d 0a 1f 8b 08 00 00 00 00 00 02 03 6d 8f 41 0e c2 30 0c 04 bf 82 f2 80 fa 1e 85 1c a8 f8 00 3f a8 82 45 10 89 6d c5 0e 82 df 53 aa 02 87 72 b3 66 b5 b3 72 50 7f a4 3b 16 16 dc 3d 6a 21 f5 ba 77 d9 4c 3c 80 a6 8c 75 d2 61 e6 ca 93 0c dc 2e f0 3e 00 d7 06 b8 18 d4 1f f8 fc 8c 61 cc 98 6e 23 13 61 b2 13 aa 30 e9 6a fc fa 0c ab f4 76 5d 3c 6e d3 e8 c5 a2 b5 8e 01 fe 04 1b b8 f8 67 fc 99 87 df 1f f1 05 c6 a0 bb bd d4 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 8cmA0?EmSrfrP;=j!wL<ua.>an#a0jv]<ng0
Aug 3, 2021 22:48:20.391555071 CEST	1173	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/EnvironmentSettings" Host: victairatu.xyz Content-Length: 144 Expect: 100-continue Accept-Encoding: gzip, deflate
Aug 3, 2021 22:48:20.436759949 CEST	1173	IN	HTTP/1.1 100 Continue
Aug 3, 2021 22:48:20.586513996 CEST	1174	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 20:48:20 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 33 65 34 0d 0a 1f 8b 08 00 00 00 00 00 02 03 bd 58 6d 8f e2 36 10 fe 2b 11 d2 4a 2d ba 25 5c b7 dd 9e 10 87 c4 4b d8 a2 5b 76 29 e1 f6 5a 29 5f 8c 33 10 17 c7 13 d9 ce 06 56 f7 e3 eb 84 84 5d f6 6e ab 12 d3 4a 88 c4 33 9e 27 e3 f1 78 fc d8 5d d5 f1 c4 23 70 4c c0 d9 c6 5c a8 8e fa d8 88 b4 4e 3a ae ab 68 04 31 51 2d 23 57 48 92 16 ca b5 9b bf b8 50 5a b8 8d 5e 57 75 06 18 ee 7a 5d 83 c2 24 8a 18 84 f6 41 6b 26 d6 6a 0e 2a 41 a1 4a e0 03 ac 86 38 49 25 2b e0 1a 6f 19 a6 5c 97 fe 90 8f 8d 81 c4 4c 81 f4 b6 1a 84 62 28 1a a5 8a 1d 30 b3 2c 6b 65 57 05 e4 4f ed f6 7b f7 8f e9 ad 5f 78 7f c9 84 d2 44 50 30 5f 22 9d 01 47 ba 81 70 88 a9 d0 72 57 a2 2c bf 19 70 cc a8 44 85 2b dd a2 18 e7 80 57 ee fb b6 eb 83 64 84 b3 27 a2 8d 0b 6e 5f 4a b2 53 0d f7 05 ec 64 76 36 c4 fb e5 5f 40 f5 cf 3d 2d 53 e8 ba cf ed 83 ea ba b7 22 5c bd d0 5d e7 3a 9f 12 51 06 4b 1d 6c 8f 84 65 a7 61 24 31 86 4a 3a 23 3a 52 e7 f0 bd d7 5d 76 94 96 66 0e 7b 17 9f 7d 6f 3e 9b df 8f 27 b7 de 45 d0 4f 92 11 d1 24 b8 45 4a 78 30 20 5a 73 68 09 d0 5d f7 60 f0 ef 4c 0b c7 59 1a 07 9f 8d e3 4e ae 38 19 e2 06 71 cd 61 8f 04 d6 38 3f 6c 3f 5c ff 68 03 36 47 12 1b 6d 70 9f 80 24 8e 6f e2 9c 11 09 c1 c9 ee 4c 49 c2 c1 d7 69 c8 b0 74 67 c6 53 65 31 be 89 64 a1 5d a4 7f f5 35 91 e5 7f 7d 94 a1 a9 0c 65 a6 da a0 44 10 a2 b6 00 78 60 8f 84 87 cc 02 e1 93 99 13 d3 a8 0f e0 71 c8 cb a4 72 ec c3 e1 25 8c 3a 33 69 c6 44 77 67 80 4b 87 f8 34 85 90 99 d1 49 22 2c 80 c6 20 24 93 ce 44 d0 c0 e7 c0 12 c1 e4 2f 81 da ef 0b 41 8c 61 ca 41 1d 8a c0 03 83 0c e4 e9 a9 60 5e 39 13 e4 46 62 9a 04 43 66 2c d0 26 b3 10 33 14 d5 a3 3e 0e 67 b0 24 36 8e fc 6e 36 20 3f 95 2b 0b 88 7b b9 64 da 6a cd 0f d1 cc 12 06 23 49 d6 56 d1 e8 c7 6c bd 0f 86 05 c8 02 25 8d 2c ec ff 24 22 84 6d f9 38 43 0d da c7 a6 3e c0 d5 75 bb f2 c2 de 9b 29 d9 ea 08 c5 95 4d 45 bb 9c 1a 22 68 33 cd 7e 92 6a c1 36 87 67 7d a4 3b 46 6d 77 f4 21 52 f3 3b 43 68 2d 8b 60 51 df ec 32 65 4a 18 6f cd d3 a0 af d1 66 35 0f 24 79 84 03 27 29 5a 97 67 c8 bc 8a 51 06 5e b8 b6 99 b0 bb 87 c9 68 d2 77 86 28 13 94 05 13 ad 44 37 30 36 6b 1f 1c 6f 6b 68 15 03 73 00 38 3d 35 35 90 f8 f4 b9 93 bb 44 e3 82 2c ff 79 57 75 df e4 e1 15 45 1f 31 45 51 86 cf 3c ff a5 b0 ec 33 5e cc 8e 68 7e de ae 54 cc ec 94 c7 c6 7b d1 4b fd 7f 42 fc 53 33 94 44 e2 ca 7c e0 22 18 81 da 68 4c be 36 5b 7a ab df 35 5b 21 d2 e6 bb e6 06 76 e6 3f 23 9c 83 36 2f 0a 20 6c 7e 6d 7f 3f d6 c7 70 48 d3 82 02 9d 0c e8 be 1e 76 15 88 1b a0 1b fc ff 4f 42 15 ed 9f e2 13 e3 9c 04 63 26 61 85 db 1a 07 87 2f 44 83 ac 67 5a d4 6f 40 51 c3 74 11 a5 66 53 34 74 41 86 35 ac cb 9d 70 42 61 4f 14 6a 40 7c 48 80 6e 55 71 de 31 8c 70 b7 ac 1b 83 3b 6f 71 d3 5f 78 ce 02 68 24 90 e3 9a 19 86 39 e0 84 6e 7e 23 59 0d bc 29 a2 a0 11 e3 a1 a1 d7 86 af d2 3c 2b 54 30 23 1c 9c 5c f5 9d 9c fc 36 03 ab dc f4 a9 04 10 c7 ab b8 94 55 3d f2 22 f5 aa 43 21 2a f5 0b 33 bf 6b f9 ba cb 41 5a f6 7a 98 dd 1d 77 c8 05 a5 ee 4b b1 a8 8e af 13 2a 59 d7 7d f3 f6 e6 4d 5d 71 25 64 b4 d5 c5 91 fb 7c 03 d5 fb 1b 9c b4 72 7e 8e 12 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 3e4Xm6+J-%\K[v)Z)_3V]nJ3'x]#pL\N:h1Q-#WHPZ^Wuz]$Ak&j*AJ8I%+o\Lb(0,keWO{_xDP0_"GprW,pD+Wd 'n_JSdv6_@=-S"\]:QKlea$1J:#:R]vf{}o>'EO$EJx0 Zsh]`LYN8qa8?l?\h6Gmp$oLiitgSe1d]5}eDx`qr%:3iDwgK4l", $ D/AaA`^9FbCf,&3>g$6n6 ?+{dj#lVl%,$"m8C>u)ME"h3~j6g};Fmw!R;Ch-`Q2eJof5$y')ZgQ^hw(D706kokhs8=55D,yWuE1 EQ<3^h~T{KBS3D|"hL6[z5[!v?#6/ l~m?pHvOBc&a/DgZo@QtfS4tA5pBaOj@|HnUq1p;oq_xh$9n~#Y)<+T0#\6U="C!*3kAZz wK*Y}M]q%d|r~0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	141.136.0.194	80	C:\Users\user\Desktop\7d9bXpW0im.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:48:30.374692917 CEST	1243	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/SetEnvironment" Host: victairatu.xyz Content-Length: 12087 Expect: 100-continue Accept-Encoding: gzip, deflate
Aug 3, 2021 22:48:30.418421984 CEST	1243	IN	HTTP/1.1 100 Continue
Aug 3, 2021 22:48:30.615509033 CEST	1255	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 20:48:30 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 37 65 0d 0a 1f 8b 08 00 00 00 00 00 02 03 45 ce 51 0a 83 40 0c 04 d0 ab c8 1e c0 fc 2f eb 7e 08 bd 80 9e 40 da 50 05 37 09 3b 69 69 6f af 2d b6 fe 0d 03 f3 98 84 78 91 27 af 6a dc bc ca 2a 88 e8 c2 ec 6e 91 08 d7 99 cb 84 76 ef a1 93 b5 5a ef f4 09 c4 c7 82 42 4e 88 bd de de 39 8d ec 3b b4 54 95 c2 e2 03 c3 54 70 98 7f d1 b9 d8 a3 2e 5f 29 50 4e f4 5b d3 79 23 6f 17 76 26 42 93 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 7eEQ@/~@P7;iio-x'j*nvZBN9;TTp._)PN[y#ov&B0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49738	141.136.0.194	80	C:\Users\user\Desktop\7d9bXpW0im.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:48:30.915970087 CEST	1256	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/GetUpdates" Host: victairatu.xyz Content-Length: 12079 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Aug 3, 2021 22:48:30.962687969 CEST	1256	IN	HTTP/1.1 100 Continue
Aug 3, 2021 22:48:31.137005091 CEST	1269	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 20:48:31 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 62 33 0d 0a 1f 8b 08 00 00 00 00 00 02 03 65 8f c1 0a c2 30 0c 86 5f 45 7a 77 99 7a 2b 5d 0f 03 f1 a2 17 45 f0 5a b6 e0 0a 5b 5b 96 cc ce b7 77 8e 3a 41 6f e1 4f f2 e5 8b 22 b9 77 0f 6c 7d c0 d5 d8 b5 8e 24 15 a2 61 0e 12 80 aa 06 3b 43 d9 94 93 37 21 f3 fd 1d de 05 60 da 00 a1 15 c9 d2 d7 4f ad 0e c8 d7 50 1b 46 3a 23 05 ef 28 f1 16 1a 63 17 86 de ce 14 f1 33 3f b4 9c ae 9b 42 94 bd 8f 84 fd 7e 64 74 64 bd 13 a9 65 17 54 8c 31 8b bb 99 b4 cd f3 0d dc 4e c7 cb ec ba b6 8e d8 b8 0a 05 68 05 ff 4a 53 f8 f1 85 ef e3 fa 05 18 8f 8c 84 05 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: b3e0_Ezwz+]EZ[[w:AoO"wl}$a;C7!`OPF:#(c3?B~dtdeT1NhJS0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 7d9bXpW0im.exe PID: 3440 Parent PID: 5652

General

Start time:	22:48:03
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\7d9bXpW0im.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7d9bXpW0im.exe'
Imagebase:	0x90000
File size:	273408 bytes
MD5 hash:	0F838CF9AC70E706AB24F4555618186C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.261102430.0000000009D70000.00000004.00000001.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: 4564 Parent PID: 3440

General

Start time:	22:48:04
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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