ID: 490256
Sample Name:
WXekVwRNtG.exe
Cookbook: default.jbs
Time: 10:15:16
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

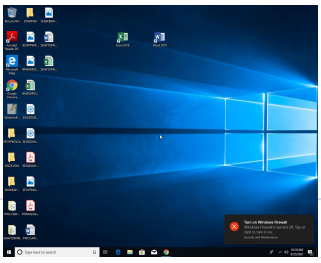
Windows Analysis Report WXekVwRNtG.exe

Overview

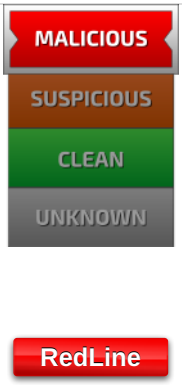
General Information

Sample Name:	WXekVwRNtG.exe
Analysis ID:	490256
MD5:	04b456ff36412c8..
SHA1:	640aec31c2ac98...
SHA256:	a7e4f1da0530887.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

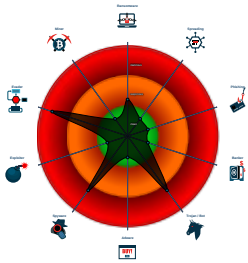


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- WXekVwRNtG.exe (PID: 4660 cmdline: 'C:\Users\user\Desktop\WXekVwRNtG.exe' MD5: 04B456FF36412C84821B0E945C24BC71)
  - conhost.exe (PID: 4344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "91.142.77.155:5469"
  ],
  "Bot Id": "10k ruzki2"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.380597703.0000000002190000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.380786166.000000000223C000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.384818345.0000000003575000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.290918132.00000000005BB000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.385834535.00000000049F0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.WXekVwRNtG.exe.2190ee8.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.WXekVwRNtG.exe.227c9d6.5.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.WXekVwRNtG.exe.227d8be.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.WXekVwRNtG.exe.2190000.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.WXekVwRNtG.exe.227c9d6.5.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)

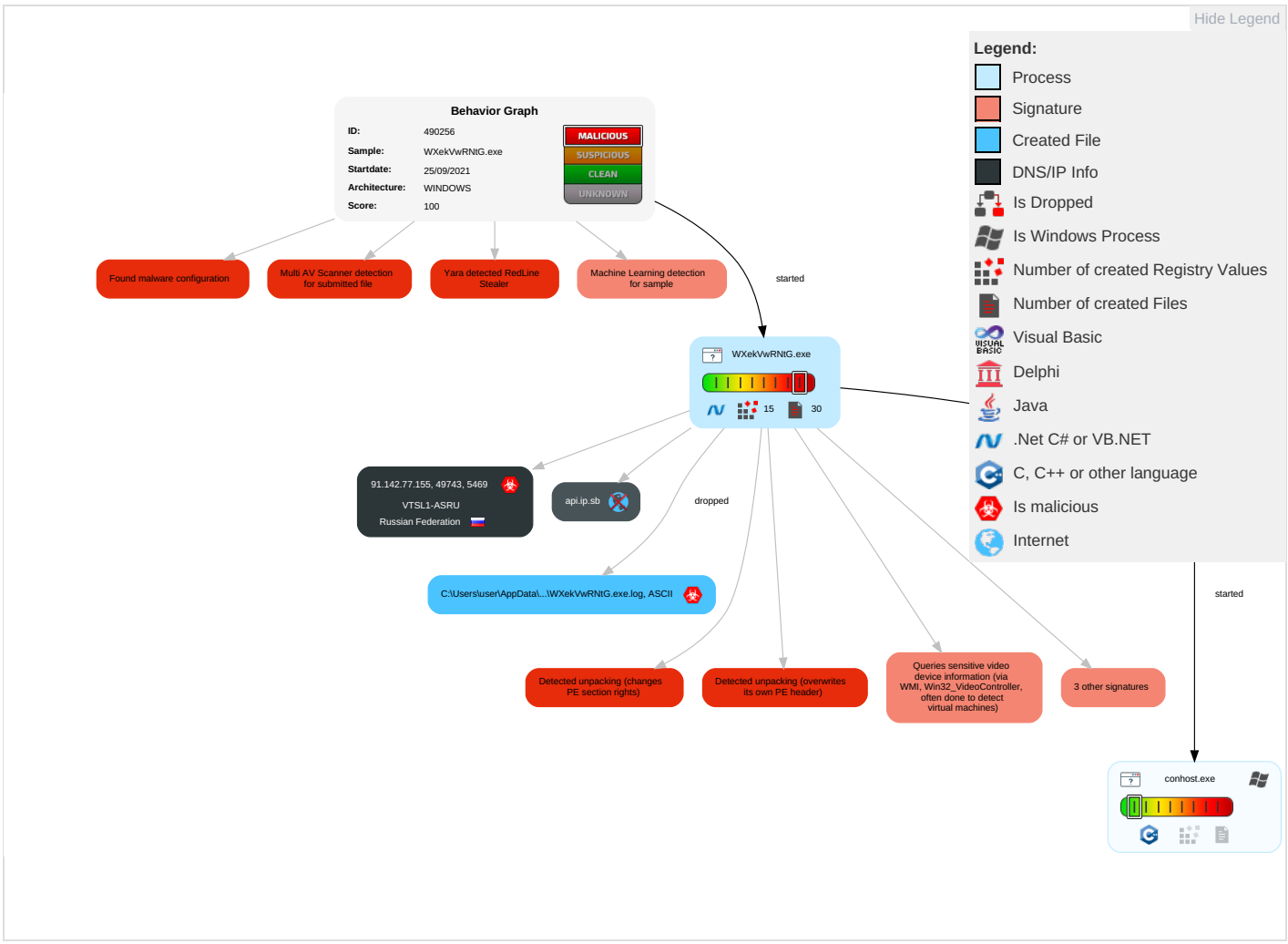
Remote Access Functionality:

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 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	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 5 1	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

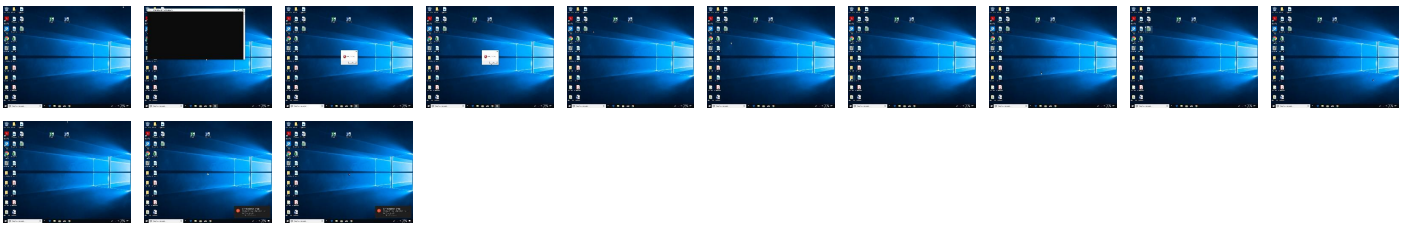
Behavior Graph



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
WXekVwRNtG.exe	72%	Virustotal		Browse
WXekVwRNtG.exe	34%	Metadefender		Browse
WXekVwRNtG.exe	93%	ReversingLabs	Win32.Ransomware.StopCrypt	
WXekVwRNtG.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://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/ConfirmResponseP	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/InitDisplayResponseP	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ip.sb	unknown	unknown	false	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.142.77.155	unknown	Russian Federation		48720	VTSL1-ASRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490256
Start date:	25.09.2021
Start time:	10:15:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WXekVwRNtG.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@2/25@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.2% (good quality ratio 11.7%) • Quality average: 84.7% • Quality standard deviation: 25%
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
10:16:44	API Interceptor	70x Sleep call for process: WXekVwRNtG.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.142.77.155	8VISLJjzRN.exe	Get hash	malicious	Browse	
	H95QHqn3LD.exe	Get hash	malicious	Browse	
	qsNXV6d1uU.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VTSL1-ASRU	8VISLJjzRN.exe	Get hash	malicious	Browse	• 91.142.77.155
	H95QHqn3LD.exe	Get hash	malicious	Browse	• 91.142.77.155
	qsNXV6d1uU.exe	Get hash	malicious	Browse	• 91.142.77.155
	f0eCiAKCaD.exe	Get hash	malicious	Browse	• 91.142.78.76
	l28uMRT0bm.exe	Get hash	malicious	Browse	• 91.142.79.92
	SecuriteInfo.com.Trojan.Win32.Save.a.17540.exe	Get hash	malicious	Browse	• 91.142.77.129
	zwAI443nmJ.exe	Get hash	malicious	Browse	• 91.142.77.129
	d5nviVgR77.exe	Get hash	malicious	Browse	• 91.142.77.129
	VUd7RUJkiC.exe	Get hash	malicious	Browse	• 91.142.77.189
	wZtYF1bDrF.exe	Get hash	malicious	Browse	• 91.142.77.189
	VibR4H3H85.exe	Get hash	malicious	Browse	• 91.142.77.189
	U6Au1ykFfo.exe	Get hash	malicious	Browse	• 91.142.77.189
	8sNtkekMJX.exe	Get hash	malicious	Browse	• 91.142.79.218
	mosoxxxHack.exe	Get hash	malicious	Browse	• 91.142.79.35
	27fb768ba20cf770d9bdc62e1403196784c903333235e.exe	Get hash	malicious	Browse	• 91.142.77.189

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	onekb0XOFQ.exe	Get hash	malicious	Browse	• 91.142.79.35
	G8y24fzAja.exe	Get hash	malicious	Browse	• 91.142.79.180
	NaCM5Ysdtq.exe	Get hash	malicious	Browse	• 91.142.79.180
	8sloK2EqDy.exe	Get hash	malicious	Browse	• 91.142.79.180
	10EqncBIA8.exe	Get hash	malicious	Browse	• 91.142.79.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WXekVwRNtG.exe.log	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKx1qH2HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKYHZHxLHqHs:PqxwWqXdq7qLqdqUqzcGYqhQnoPtIxHt
MD5:	AC1D59E5183C5AA98A6D7649ADF5A0CD
SHA1:	21E7AB307B697EC5C3A3D8C4D61ADA8ADC946C66
SHA-256:	6EA269BF1E1B8D694C1E177CA04CC944C6A6F251A70635CD8A0A62563745D357
SHA-512:	E9917B7F991E780418992C1A5D271584E39B750D75FCB1573724B7FAE9BAEBD36C76177847DD28BD7912CBAD61617FBB6756B924506E242D2F82D0B020F4F1B4
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.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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=b77a5c5

C:\Users\user\AppData\Local\Temp\tmp225B.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp225C.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831

C:\Users\user\AppData\Local\Temp\tmp225C.tmp	
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\tmp4101.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp4121.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp4122.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp4122.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4123.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp4162.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp4163.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp5F8B.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584

C:\Users\user\AppData\Local\Temp\tmp5F8B.tmp	
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\tmp5F8C.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp5FBC.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp5FBD.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp5FBD.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5FBE.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp5FBF.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp7D6A.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp7D6B.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp7D6B.tmp	
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp9AE7.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp9B17.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmp9B18.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE

C:\Users\user\AppData\Local\Temp\tmp9B18.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp9B19.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmpC33F.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmpC340.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69422273140364
Encrypted:	false
SSDEEP:	24:hdGRma8y0UOkmVb01yh9qfT+PsSMxto3vIcMhrzxYWSDHtj:hdGRma6bRh9rsFE/uhrOWSDHh
MD5:	A686C2E2230002C3810CB3638589BF01
SHA1:	4B764DD14070E52A2AC0458F401CDD5724E714FB
SHA-256:	38F526D338AC47F7C2CAB7AB654A375C87E51CC56B4FA09A7C5769E2FB472FFC
SHA-512:	1F2AA9D4B55B52C32EF0C88189256562B16DF13EEA0564BD7B47E45CC39279F39823033ADF95BBD9A50B4F35E417E418C4D20BBE14EF425EFF7134ECE05BEB3 F
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpC340.tmp	
Preview:	SUAVTZKNFLPDUIKIPSQJDVGAPGXKDOHYHNOWHLTUYHUBPZNAGHXWSRGELNTTLWSOVKHBKQEKGENMQDFUYQEFPUMFVGFHNHBEYAAJVHSIYLSLGV ZSSKYNEFOJGJXPWCGXOBRZVXDWDDKKLDGWVLNCMOJKBSBYFMTKILZOONEGLZWORUNOTXJNOTGXQTUBOXEFHVICNNYYHMRGCLTZLWQODATYJZBG FVEMSABDUIKNKVRGQOHHCSHZAJIYWZLGGZOOEOQBTEAFTXBQJIHRZBDRPFDGHVFGYZEIHFYVBPAXJYSLOTRVHEFEEWXUGJCOLFXEKSPFHBKQEH GPZADNNCAUYCTEDLFKZMZOQOADUCTDIOYKELVKGABHEMOSAYPWUUKTZHQNEQWLFATTPCULHLMBMEQVAXDFQNQLMLVOFTUTWLMJNL VNCRHTWUTJEEORGWISXALHDTNXRCWVMZRUEMSVOJYMENRHGVXXMGLOWYRFKZLPBZQMETPESMZPCJGYXVQSMCJXYEMMNKLPIXGOXO MQNYCFAEVPXDGOFEGSLWKBUOLRKXGTWDFUVGYFTOWQZAOIMQUZEELMCQWKUBEWGFDVXSXNGHPJNVDQHMPSSIFZTQLVBBHZOEGNPD AWAYLIRBWZHXRAXBBESYNRIRINAKLQMELNYRHRPKDBUCNSZOVHNTBCUYDQTGFWZJUCUZBHHXHQHKWOWTEWLUGGGWHIHCWZLLJPDFVDICZBBLFS ECTLMQBKCPCHANOICKIUSVAJTYQOIUWRGVAFOFTMIHARUUCNGBLVFIKMTTGPYXNEVGLPMZDMIQDQOLIEFHNZYMZTCDOHBNQLNVLXRUXMGYCVOJ DBWPSJKMFMEDBEMXULQBRVRKPYNUACCXNPGFEMPXDXNEIPTKGSKUMVFSLCTJFHNFATCDKSZWKYMVQNTVHCOAJXDUTJZESFLKTQOGREXBTBVBGL DYJYDTNEAQDFRTXMJIHJCCTPUDZLNKNEABFQYCDL

C:\Users\user\AppData\Local\Temp\tmpC370.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.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\tmpC371.tmp	
Process:	C:\Users\user\Desktop\WXekVwRNtG.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69422273140364
Encrypted:	false
SSDEEP:	24:hdGRma8y0UOkmVb01yh9qfT+PsSMxto3vIcMhrzxYWSDHtj:hdGRma6bRh9rsFE/uhrOWSDHh
MD5:	A686C2E2230002C3810CB3638589BF01
SHA1:	4B764DD14070E52A2AC0458F401CDD5724E714FB
SHA-256:	38F526D338AC47F7C2CAB7AB654A375C87E51CC56B4FA09A7C5769E2FB472FFC
SHA-512:	1F2AA9D4B55B52C32EF0C88189256562B16DF13EEA0564BD7B47E45CC39279F39823033ADF95BBD9A50B4F35E417E418C4D20BBE14EF425EFF7134ECE05BEB3F
Malicious:	false
Preview:	SUAVTZKNFLPDUIKIPSQJDVGAPGXKDOHYHNOWHLTUYHUBPZNAGHXWSRGELNTTLWSOVKHBKQEKGENMQDFUYQEFPUMFVGFHNHBEYAAJVHSIYLSLGV ZSSKYNEFOJGJXPWCGXOBRZVXDWDDKKLDGWVLNCMOJKBSBYFMTKILZOONEGLZWORUNOTXJNOTGXQTUBOXEFHVICNNYYHMRGCLTZLWQODATYJZBG FVEMSABDUIKNKVRGQOHHCSHZAJIYWZLGGZOOEOQBTEAFTXBQJIHRZBDRPFDGHVFGYZEIHFYVBPAXJYSLOTRVHEFEEWXUGJCOLFXEKSPFHBKQEH GPZADNNCAUYCTEDLFKZMZOQOADUCTDIOYKELVKGABHEMOSAYPWUUKTZHQNEQWLFATTPCULHLMBMEQVAXDFQNQLMLVOFTUTWLMJNL VNCRHTWUTJEEORGWISXALHDTNXRCWVMZRUEMSVOJYMENRHGVXXMGLOWYRFKZLPBZQMETPESMZPCJGYXVQSMCJXYEMMNKLPIXGOXO MQNYCFAEVPXDGOFEGSLWKBUOLRKXGTWDFUVGYFTOWQZAOIMQUZEELMCQWKUBEWGFDVXSXNGHPJNVDQHMPSSIFZTQLVBBHZOEGNPD AWAYLIRBWZHXRAXBBESYNRIRINAKLQMELNYRHRPKDBUCNSZOVHNTBCUYDQTGFWZJUCUZBHHXHQHKWOWTEWLUGGGWHIHCWZLLJPDFVDICZBBLFS ECTLMQBKCPCHANOICKIUSVAJTYQOIUWRGVAFOFTMIHARUUCNGBLVFIKMTTGPYXNEVGLPMZDMIQDQOLIEFHNZYMZTCDOHBNQLNVLXRUXMGYCVOJ DBWPSJKMFMEDBEMXULQBRVRKPYNUACCXNPGFEMPXDXNEIPTKGSKUMVFSLCTJFHNFATCDKSZWKYMVQNTVHCOAJXDUTJZESFLKTQOGREXBTBVBGL DYJYDTNEAQDFRTXMJIHJCCTPUDZLNKNEABFQYCDL

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.201715742815139

General

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:	WXekVwRNtG.exe
File size:	326656
MD5:	04b456ff36412c84821b0e945c24bc71
SHA1:	640aec31c2ac988d7bc2ba39accd1399d68c7e48
SHA256:	a7e4f1da0530887fb3c60141d8263cc9c92474067f9f8c6b9b65633a72bd87ce
SHA512:	44099256bdfb87662b5eb13b9d7de9ca09565d6c162d6a9cf6cf90fdf32c75f60cb32149fba17778e592f7b4211eeb5cf604299b28c9f6b1f9196f2e6d6a3048
SSDEEP:	6144:wNZQtZa/fEK5uuWyF9L12P0TKIbywJLSjyYWf67fDwdfMP9UGLL8:qZb/fEK5uzIL12sWImzjyYWy7fyUPWK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..u(..&(..&(..&6.~&9..&6.h&F..&6.o&...&.o.&-..&(..&...&6.a&)..&6..&)..&6.z&)..&Rich(..&.....PE..L....._.....

File Icon

Icon Hash:	aedaae9ec6a68aa4

Static PE Info

General

Entrypoint:	0x401fd0
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:	0x5FBCAC8C [Tue Nov 24 06:47:40 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2d3e8f1de619588f819136537821e72a

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1be40	0x1c000	False	0.462602887835	data	6.28761952965	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x8a6e	0x8c00	False	0.307310267857	data	4.74858051119	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x26000	0x3183c	0x23a00	False	0.96367872807	data	7.91574031298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x58000	0x38b8	0x3a00	False	0.672009698276	data	5.92959015572	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	0x5c000	0x3774	0x3800	False	0.371233258929	data	3.85690026782	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
Sami Lappish	Finland	
Sami Lappish	Norway	
Sami Lappish	Sweden	
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 10:16:43.104506016 CEST	192.168.2.3	8.8.8.8	0x1dfd	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Sep 25, 2021 10:16:43.137342930 CEST	192.168.2.3	8.8.8.8	0x1e4a	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 10:16:43.122579098 CEST	8.8.8.8	192.168.2.3	0x1dfd	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 25, 2021 10:16:43.158360958 CEST	8.8.8.8	192.168.2.3	0x1e4a	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: WXekVwRNtG.exe PID: 4660 Parent PID: 672

General

Start time:	10:16:11
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\WXekVwRNtG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\WXekVwRNtG.exe'
Imagebase:	0x400000
File size:	326656 bytes
MD5 hash:	04B456FF36412C84821B0E945C24BC71
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: 00000000.00000002.380597703.0000000002190000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.380786166.000000000223C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.384818345.0000000003575000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.290918132.00000000005BB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.385834535.000000000049F0000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4344 Parent PID: 4660

General

Start time:	10:16:11
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	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