ID: 1352257
Sample Name: WolferVPN.exe
Cookbook: default.jbs
Time: 22:03:31
Date: 02/12/2023
Version: 38.0.0 Ammolite

Table of Contents

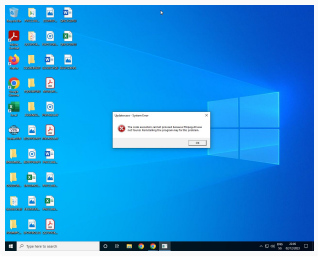
Windows Analysis Report

WolferVPN.exe

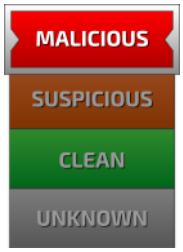
Overview

General Information

Sample Name:	WolferVPN.exe
Analysis ID:	1352257
MD5:	6434ceafa88a3..
SHA1:	700b43db6881...
SHA256:	db230e271893...
Tags:	BbyStealer exe
Infos:	



Detection

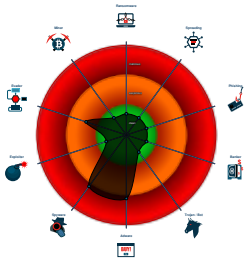


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dom...
- Multi AV Scanner detection for drop...
- Drops PE files to the startup folder
- Drops large PE files
- Tries to harvest and steal browser in...
- Uses 32bit PE files
- Drops files with a non-matching file ...
- Queries the volume information (nam...
- Drops PE files
- Very long cmdline option found, this...
- PE file contains sections with non-s...
- Creates a start menu entry (Start M...

Classification



Process Tree

- **System is w10x64**
- WolferVPN.exe (PID: 1416 cmdline: C:\Users\user\Desktop\WolferVPN.exe MD5: 6434CEAFA88A3AFA1F8351BC6890B2A5)
- WolferVPN.exe (PID: 6732 cmdline: "C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe" MD5: 4AD8066DFB8E65195E5733DDFD8A1AC7)
  - WolferVPN.exe (PID: 2328 cmdline: "C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe" --type=gpu-process --user-data-dir="C:\Users\user\AppData\Roaming\WolferVPN" --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=1680 --field-trial-handle=1684,i,16203821050471540 44,16004179749874181730,262144 --disable-features=SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand /prefetch:2 MD5: 4AD8066DFB8E65195E5733DDFD8A1AC7)
  - cmd.exe (PID: 7072 cmdline: C:\Windows\system32\cmd.exe /d /s /c "tasklist" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 1224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - tasklist.exe (PID: 2708 cmdline: tasklist MD5: D0A49A170E13D7F6AEBBEFED9DF88AAA)
  - WolferVPN.exe (PID: 1616 cmdline: "C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --user-data-dir="C:\Users\user\AppData\Roaming\WolferVPN" --mojo-platform-channel-handle=2204 --field-trial-handle=1684,i,16203821050471540 44,16004179749874181730,262144 --disable-features=SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand /prefetch:8 MD5: 4AD8066DFB8E65195E5733DDFD8A1AC7)
  - cmd.exe (PID: 6536 cmdline: C:\Windows\system32\cmd.exe /d /s /c "tasklist" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - tasklist.exe (PID: 4800 cmdline: tasklist MD5: D0A49A170E13D7F6AEBBEFED9DF88AAA)
- Updater.exe (PID: 1948 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe" MD5: 4AD8066DFB8E65195E5733DDFD8A1AC7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

System Summary

Drops large PE files

Boot Survival

Drops PE files to the startup folder

Stealing of Sensitive Information

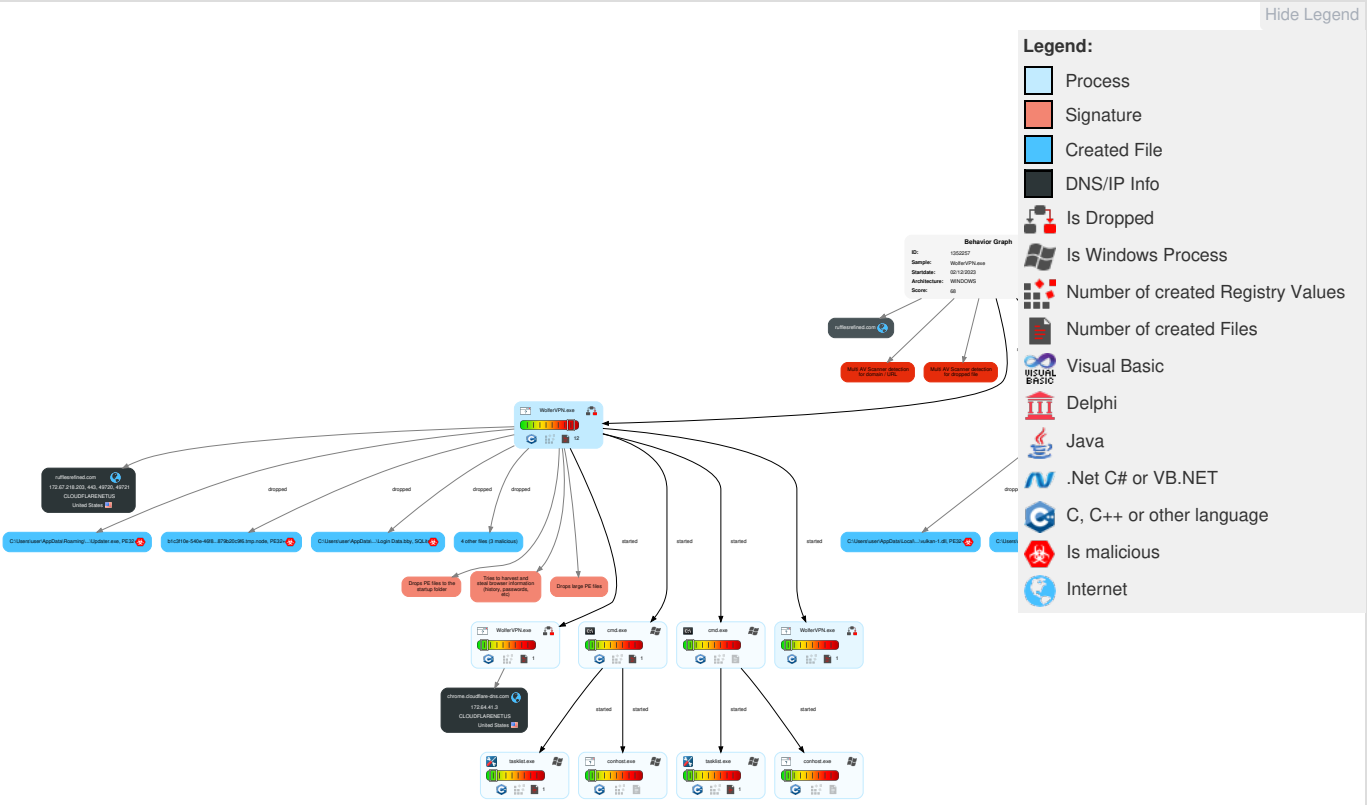
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact	Resource Development	Reconnaiss
Valid Accounts	1 Windows Management Instrumentation	1 Windows Service	1 Windows Service	1 1 Masquerading	1 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 1 Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Abuse Accessibility Features	Acquire Infrastructure	Gather Victim Identity Information
Default Accounts	1 Command and Scripting Interpreter	1 2 Registry Run Keys / Startup Folder	1 1 Process Injection	1 1 Process Injection	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	SIM Card Swap	Obtain Device Cloud Backups	Network Denial of Service	Domains	Credentials
Domain Accounts	At	Logon Script (Windows)	1 2 Registry Run Keys / Startup Folder	Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Application Layer Protocol			Data Encrypted for Impact	DNS Server	Email Addresses
Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	1 2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Traffic Duplication	Protocol Impersonation			Data Destruction	Virtual Private Server	Employee Names

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact	Resource Development	Reconnaiss
Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	2 3 System Information Discovery	SSH	Keylogging	Scheduled Transfer	Fallback Channels			Data Encrypted for Impact	Server	Gather Victim Network Information

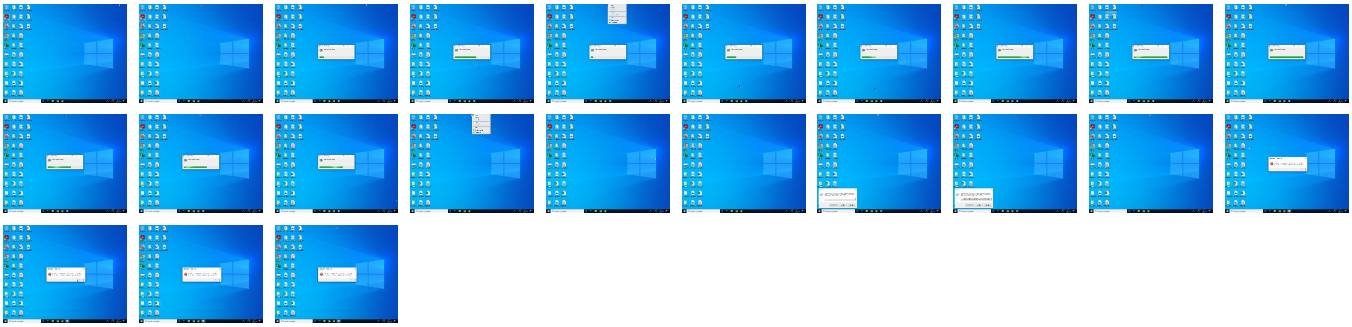
Behavior Graph

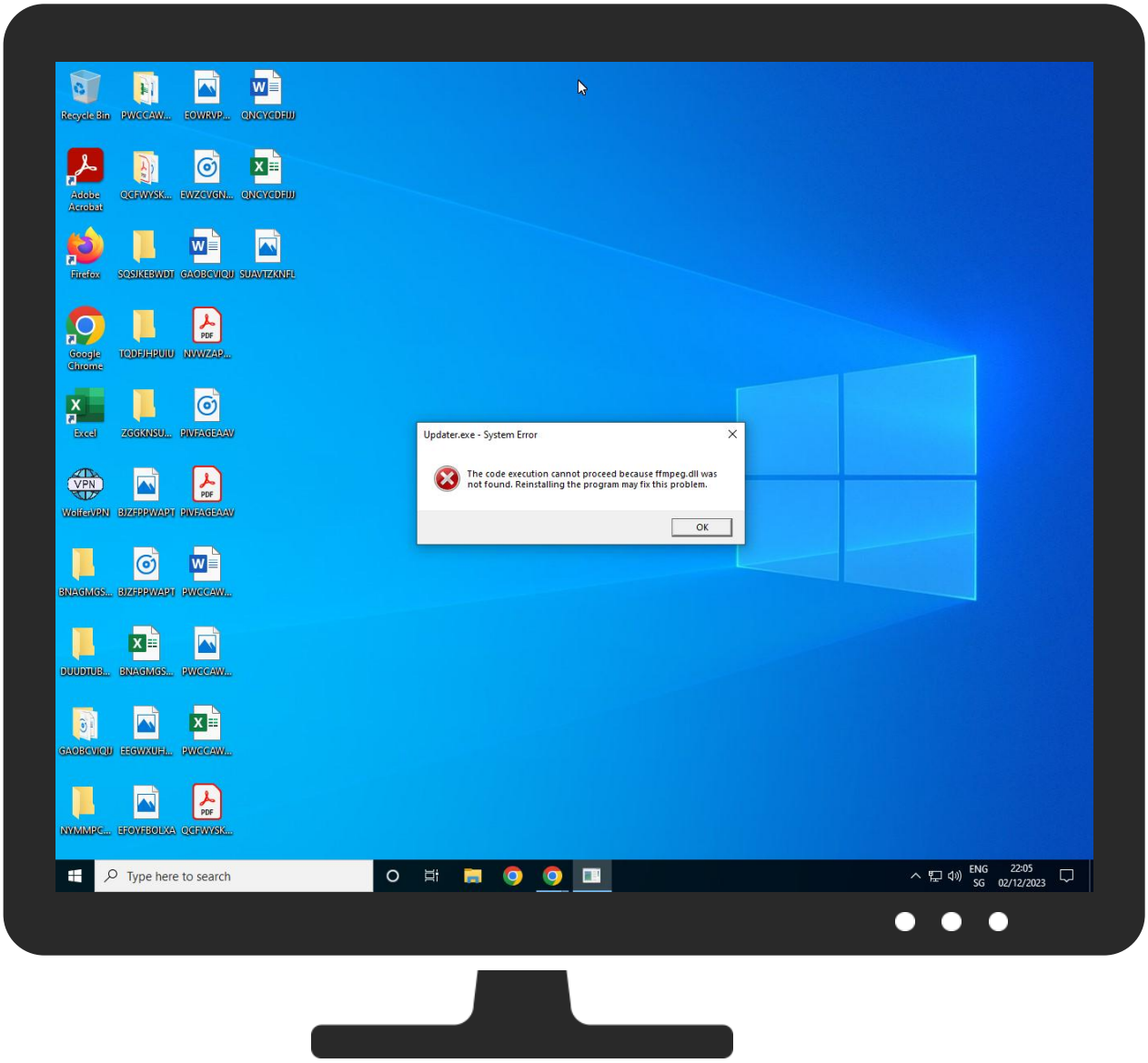


Screenshots

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
WolferVPN.exe	0%	ReversingLabs		
WolferVPN.exe	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\WolferVPN\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\d3dcompiler_47.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\WolferVPN\ffmpeg.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\ffmpeg.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\WolferVPN\libEGL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\libEGL.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\WolferVPN\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\libGLESv2.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Programs\WolferVPN\vulkan-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\WolferVPN\vulkan-1.dll	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\8aa2ec43-5e03-40f0-b44b-d7dcf4df059c.tmp.node	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\8aa2ec43-5e03-40f0-b44b-d7dcf4df059c.tmp.node	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\b1c3f10e-540e-46f8-9bee-83879b20c9f6.tmp.node	41%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\b1c3f10e-540e-46f8-9bee-83879b20c9f6.tmp.node	40%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\WolferVPN.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\ffmpeg.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\libEGL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\resources\elevate.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\vk_swiftshader.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\vulkan-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\SpiderBanner.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\StdUtils.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\nsis7z.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
rufflesrefined.com	17%	Virustotal		Browse
chrome.cloudflare-dns.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pajhome.org.uk/crypt/md5	0%	URL Reputation	safe	
http://https://v8.dev/docs/embed#exceptions)	0%	Virustotal		Browse
http://https://v8.dev/docs/embed#interceptors).	0%	Virustotal		Browse
http://https://v8.dev/docs/embed#interceptors).	0%	Avira URL Cloud	safe	
http://stuartk.com/jszip	0%	Avira URL Cloud	safe	
http://https://v8.dev/docs/embed#exceptions)	0%	Avira URL Cloud	safe	
http://www.netdealing.com	0%	Virustotal		Browse
http://www.netdealing.com	0%	Avira URL Cloud	safe	
http://digitalbazaar.com/	0%	Avira URL Cloud	safe	
http://stuartk.com/jszip	0%	Virustotal		Browse
http://digitalbazaar.com/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rufflesrefined.com	172.67.218.203	true	false	• 17%, Virustotal, Browse	unknown
chrome.cloudflare-dns.com	172.64.41.3	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.netdealing.com	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

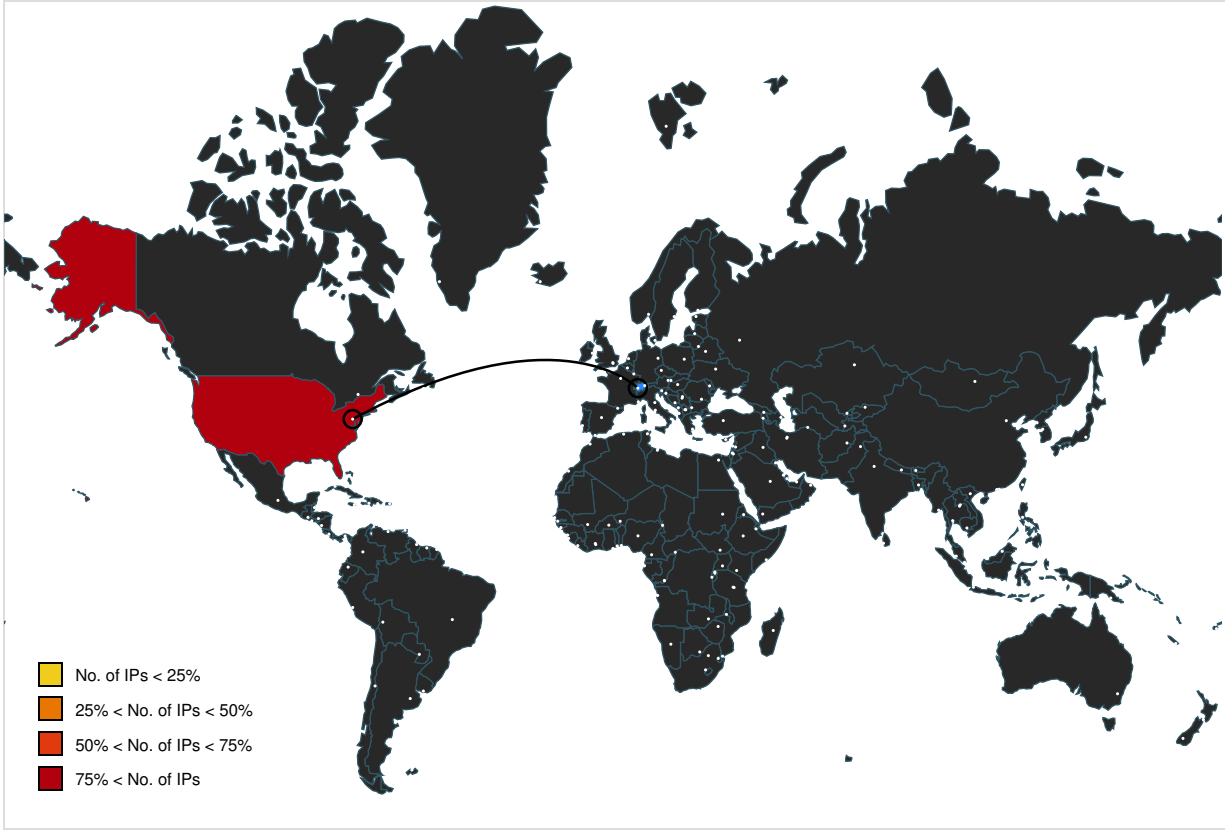
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://v8docs.nodesource.com/node-8.16/dc/d0a/classv8_1_1_value.html#a08fba1d776a59bbf6864b25f9152c	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/TooTallNate	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/nodejs/node/blob/v10.8.0/lib/internal/errors.js	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/mafintosh/mkdirp-classic.git	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#a6f76b2ed605cb8f9185b92de0033	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/d54/classv8_1_1_function.html#a9c3d0e4e13ddd7721fce238aa5	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d9/d28/classv8_1_1_message.html#adbe46c10a88a6565f2732a2d2ad	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://seclists.org/fulldisclosure/2009/Sep/394	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/PeculiarVentures/webcrypto-core.git	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/v8/v8/wiki/Embedder%27s%20Guide#handles-and-garbage-collection).	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/de/d73/classv8_1_1_non_copyable_persistent_traits.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#ab7b7245442ca6de1e1c145ea3fd6	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.rsa.com/rsalabs/node.asp?id=2125	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/nodejs/string_decoder	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8.dev/docs/embed#interceptors).	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/PeculiarVentures/webcrypto-core#readme	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/da/da5/classv8_1_1_script_compiler.html#a93f5072a0db55d881b9	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://tools.ietf.org/html/rfc8410#section-10.3	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.patreon.com/feross	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/TooTallNate/util-deprecate	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/crypto-browserify/md5.js.git	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/digitalbazaar/forge	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://sqlite.org/wal.html#ckpt	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/dda/classv8_1_1_isolate.html#aabd223436bc1100a787dadaa024	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/dchest/tweetnacl-js	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/kkoopa	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/dda/classv8_1_1_isolate.html#a542d67e85089cb3f92aadf032f9	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d5f/classv8_1_1_object_template.html#a5e9612fc80bf6db8f2d	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://semver.org/	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#af743b7ea132b89f84d34d164d066	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/d54/classv8_1_1_function.html#ae477558b10c14b76ed00e8dbab	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#a2565f03e736694f6b1e1cf22a0b4	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/dda/classv8_1_1_isolate.html#ad6a2a02657f5425ad460060652a	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/da/d6a/classv8_1_1_exception.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/electron/node-abi#readme	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://digitalbazaar.com/	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://datatracker.ietf.org/doc/html/rfc7468#section-7	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://nodejs.org/api/addons.html#addons_wrapping_c_objects)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d3/d95/classv8_1_1_handle_scope.html).	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d8/d06/classv8_1_1_weak_callback_info.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/String/endsWith	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/dominictarr/varstruct.git	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/dda/classv8_1_1_isolate.html#a045d7754e62fa0ec72ae6c259b2	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://sqlite.org/lang_savepoint.html	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://stackoverflow.com/a/1068308/13216	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d4/dca/classv8_1_1_persistent_base.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#ab7a92b4dcf822bef72f6c0ac6fea	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/fanatid)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/digitalbazaar/forge/blob/master/lib/asn1.js#L542	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-0.12/db/d85/classv8_1_1_object.html#acfbdfd7427b516ebdb5c47c4df5e	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://developer.mozilla.org/en-US/docs/JavaScript/Reference/Operators/Bitwise_Operators	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/kjur/jsjws/blob/master/rsa.js:	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.openssl.org	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/mkrufky	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d9/db3/classv8_1_1_string_1_1_external_one_byte_string_resou	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://aka.ms/opensource/security/bounty)	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/RyanZim/universalify#readme	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d5f/classv8_1_1_object_template.html#a33b3ebd7de641f6cc64	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/trevnorris	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#a8700b1862e6b4783716964ba4d5e	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.unicode.org/copyright.html	WolferVPN.exe, 00000000.00000003.2248611287.0000000005650000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://developer.mozilla.org/en-US/docs/Web/API/window.crypto.getRandomValues	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/cryptocoinjs/base-x	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/RyanZim/universalify.git	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://stuartk.com/jszip	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://v8.dev/docs/embed#exceptions)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#ace1769b0f3b86bfe9fda10109163	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d2/db3/classv8_1_1_string.html#a5264d50b96d2c896ce525a734dc1	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d4/dc6/classv8_1_1_try_catch.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/da/d6f/classv8_1_1_j_s_o_n.html#a936310d2540fb630ed37d3ee3ff	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/agnat	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/nodejs/nan#wg-members--collaborators	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/dda/classv8_1_1_isolate.html#aeb420b690bc2c216882d6fdd00d	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://pajhome.org.uk/crypt/md5	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/inspiredware/napi-build-utils#readme	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://unicode.org/reports/tr15/	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.joyent.com	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d5f/classv8_1_1_object_template.html#ad605a7543cfbc5dab54	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#ad8b80a59c9eb3c1e6c3cd6c84571	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d2/d78/classv8_1_1_persistent.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d5/dda/classv8_1_1_isolate.html#a5f72c7cda21415ce062bbe5c58a	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d9/d28/classv8_1_1_message.html#a60ede616ba3822d712e44c7a744	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/sponsors/feross	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/rvagg	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/xamarin)	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#a50d571de50d0b0dfb28795619d07	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/crypto-browserify/md5.js	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.info-zip.org/FAQ.html#backslashes	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://hackage.haskell.org/package/base/docs/Data-Maybe.html.	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/mafintosh/pump	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://sindresorhus.com	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.gnu.org/licenses/gpl-2.0-standalone.html	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/mafintosh/tar-stream.git	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-4.8/d3/d32/classv8_1_1_array.html#a1d3a878d4c1c7cae974dd50a163924	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/dd/d0d/classv8_1_1_function_callback_info.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/d7/dc5/classv8_1_1_property_callback_info.html)	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://v8docs.nodesource.com/node-8.16/db/d85/classv8_1_1_object.html#a169f2da506acbec34deadd9149a1	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/mafintosh/end-of-stream	WolferVPN.exe, 00000000.00000003.2260475006.0000000005250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://github.com/inspiredware/napi-build-utils#napi-build-utils).	WolferVPN.exe, 00000000.00000003.2260205445.0000000004A50000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.218.203	rufflesrefined.com	United States		13335	CLOUDFLARENETUS	false
172.64.41.3	chrome.cloudflare-dns.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	38.0.0 Ammolite
Analysis ID:	1352257
Start date and time:	2023-12-02 22:03:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	18
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	WolferVPN.exe
Detection:	MAL
Classification:	mal68.adwa.spyw.winEXE@17/107@3/2
EGA Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 172.253.122.94
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, www.gstatic.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:04:43	API Interceptor	14x Sleep call for process: WolferVPN.exe modified
22:05:01	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

(copy)

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	JSON data
Category:	dropped

Size (bytes):	413
Entropy (8bit):	5.622417211407826
Encrypted:	false
SSDEEP:	12:YKWSg99rrt+UWikSdiO8CXBETpFFELTiJwrTM+Yi:YKWfrrtRKSIWxETpYUap
MD5:	2B7F19F2FC201FE27C212FD1632F5DDA
SHA1:	88D959B59438F87DCCE44257EF05F9F38FF4C407
SHA-256:	CEF41FE2D16205892A1DF22A2C88832466ED75A076638D012BD29A5959E5E820
SHA-512:	26F89D0351A7E37A1530056FFE60909A3384B5F3968DF3D5CFB7AEB6D72179DDE3479F69A3C2C82532CD3FF92994DF2B31B9F020ECED448C1EA796058FE9329
Malicious:	false
Reputation:	low
Preview:	{"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABSjLU7zYUkRIPDR3IKCUEYEAAAABIAAABDAGgAcgBvAG0AaQB1AG0AAAAQZgAAAAEAACAAAAAeMaPdqvU3Xbi0T02ZH5wtD6AJW8AlOVF7SGt257dJiAAAAAAOgAAAAIAACAAAACrL85c9u6lBijPt91xlpUc9rxSaZ6fliLLRvB9E3wFYTAAAACALkhxWEeKdqOMLlkOrfGrQrslxxZx8G5wcvHtbGo2wEGeS1HHQN+nCHXfGbnY7TdAAAAAkxRJQLgHWJXOsC1ikz3GGcODiAJQkgw7OiQcZmYu6NaIuMFYO+KW4VjEkWZcTkFNCwB7H51Z8RKSyYH/uoRqlQ==}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bby

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.bby

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 6, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 6
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8508558324143882
Encrypted:	false
SSDEEP:	24:TLIF1kwNbXYFpFNYcw+6UwcQVXH5fBaJvWKC0ABndzGrW7swaE:TxFawNLopFgU10XJBaEKQxdgQsw
MD5:	933D6D14518371B212F36C3835794D75
SHA1:	92D056D912B3C0260D379330D3CC0359B57A322B
SHA-256:	55390EE61FB85370A8A7F51A8DD5374F7B1801D1D7DF09D6A90CDD74ED6E7D1E
SHA-512:	EAC706D8A579500EADA26FB9883E1F3CE9112A03F38EE78B11B393AB0A3285945F8E06EB406BFC17D1CB540F840E435E515FABFC265399CE6F5193980FDE3F2C
Malicious:	**true**
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bby

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136471148832945
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c1/k4:MnlyfnGtxnfVuSVumEH1s4

MD5:	37B1FC046E4B29468721F797A2BB968D
SHA1:	50055EF1C50E4C1A7CCF7D00620E95128E4C448B
SHA-256:	7BBD5DFC9026E0D477B027B9A2A3F022F2E72FC9B4E05E697461A00677AE8EFD
SHA-512:	1D8A0F0AE76E5A1CF131F6D2C5156EA4204449942210EF029D5B018464355DBF94E2D8ABD6A5A9CDFE4271DCD22703BF26ECE8FEE902E122184680F1BB00114 9
Malicious:	**true**
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data.bby

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 2, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8745947603342119
Encrypted:	false
SSDEEP:	96:aZ8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:W8yLG7IwRWf4
MD5:	378391FDB591852E472D99DC4BF837DA
SHA1:	10CB2CDAD4EDCCACE0A7748005F52C5251F6F0E0
SHA-256:	513C63B0E44FFDE2B4E511A69436799A8B59585CB0EB5CCFDA7A9A8F06BA4808
SHA-512:	F099631BEC265A6E8E4F8808270B57FFF28D7CBF75CC6FA046BB516E8863F36E8506C7A38AD682132FCB1134D26326A58F5B588B9EC9604F09FD7155B2AEF2D
Malicious:	**true**
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies.bby

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data.bby

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false

Preview:	SQLite format 3.....@ .....Y.....7.....j.....W.....

C:\Users\user\AppData\Local\Programs\WolferVPN\LICENSE.electron.txt

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1096
Entropy (8bit):	5.13006727705212
Encrypted:	false
SSDEEP:	24:36DiJHxRHuyPP3GtIHw1Gg9QH+sUW8Ok4F+d1o36qjFD:36DiJzfPvGt7ICQH+sfIte36AFD
MD5:	4D42118D35941E0F664DDDBD83F633C5
SHA1:	2B21EC5F20FE961D15F2B58EFB1368E66D202E5C
SHA-256:	5154E165BD6C2CC0CFBCD8916498C7ABAB0497923BAFCD5CB07673FE8480087D
SHA-512:	3FFBBA2E4CD689F362378F6B0F6060571F57E228D3755BDD308283BE6CBBEF8C2E84BEB5FCF73E0C3C81CD944D01EE3FCF141733C4D8B3B0162E543E0B9F3E63
Malicious:	false
Preview:	Copyright (c) Electron contributors.Copyright (c) 2013-2020 GitHub Inc...Permission is hereby granted, free of charge, to any person obtaining.a copy of this software and associated documentation files (the."Software"), to deal in the Software without restriction, including.without limitation the rights to use, copy, modify, merge, publis h,.distribute, sublicense, and/or sell copies of the Software, and to.permit persons to whom the Software is furnished to do so, subject to.the following conditions:..The above copyright notice and this permission notice shall be.included in all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", W ITHOUT WARRANTY OF ANY KIND,.EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF.MERCHANTABILITY, FITNESS FOR A PAR TICULAR PURPOSE AND.NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE.LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION.OF CONTRACT, TORT OR OTHERWISE, ARISIN

C:\Users\user\AppData\Local\Programs\WolferVPN\LICENSES.chromium.html

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	8245721
Entropy (8bit):	4.70761969468716
Encrypted:	false
SSDEEP:	24576:dbTj6ck6f5kVWS6RqLsWN3Omfpe666A6f6X6TTHW9GqpaE:tEx/i
MD5:	0E3E4362F785AFF0B9E1852B1064C0F1
SHA1:	A42CCB51E72BDCB5BB905A62EFAA28857DEF3A17
SHA-256:	BD3EE49A5AB19D15DDC44B421B0BDEFCE587790786989AE77CF3DDF1E6A2BA8D
SHA-512:	193B57EFC5F5971FBD9E4EA1A80B34AADCC2A814FF49C4C06AFE972BF327E98FF0498217A8BDEF984B10FDEC6E7858A6FB88C0B14936E0C6B404387A426B87F2
Malicious:	false
Preview:	Generated by licenses.py; do not edit. --><!doctype html>.<html>.<head>.<meta charset="utf-8">.<meta name="viewport" content="width=device-width">.<meta name ="color-scheme" content="light dark">.<title>Credits</title>.<link rel="stylesheet" href="chrome://resources/css/text_defaults.css">.<link rel="stylesheet" href="chrome:/ /credits/credits.css">.</head>.<body>.Credits.Print.<div s tyle="clear:both; overflow:auto;"> Chromium <3s the following projects -->. .2-dim General Purpose FFT (Fast Fourier/C osine/Sine Transform) Package.homepage.<input type= "checkbox" hidden id="0">.<label class="show" for="0" tabindex="0"></label>. .<pre>Copyright(C) 1997,2001 Takuya OOURA (email: ooura@kurims. kyoto-u.ac.jp)..You may us

C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	163343360
Entropy (8bit):	6.732960636432368
Encrypted:	false
SSDEEP:	1572864:VOehMi9HmQapOF/wcuOG/KTlWoqYtUMogmhQXoqAfIgrWAdBb9pTHPe3HdYYGQc1:4ZK9PUddCvs
MD5:	4AD8066DFB8E65195E5733DDFD8A1AC7
SHA1:	8225752BBC6C6720F92B8890117A76576AB5D951
SHA-256:	BB3651F02D8CDBC962EC910EC5E6DE3BAD9DD94CBB811DA098116E19C4BE7C0F
SHA-512:	BA5951A9455A06060AA349F66D2AF97227E5617B2D6867CA3AB0AA1082D3528D0AE43481F0C8FFD489A84B748CCCC88FE5AAD805F753E339B691F836B2905C5D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke.....".....f.....j%.....@.....`..... .....[..'...^.h.....'A.....L..p.Q.....PzQ.(... ...@.....^.`....@[.....text..... ..`.rdata....n.....n.....@. .@.data.....C...b.....b.....@....pdata...'A.....(A...j.....@..@.00cfg..0.....@..@.gxfg...pA.....B.....@..@.retplne..... .....rodata... ...0..... ..... ..`.tls.....P.....2.....@...CPADinfo8....`.....8.....@...LZMADEC.....p.....:..... ..`_RDATA..\.....L.....@..@malloc_h..... .N..... ..`.rsrc.....P.....@..@.reloc...L.....N.....@..B.....

C:\Users\user\AppData\Local\Programs\WolferVPN\chrome_100_percent.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	135956
Entropy (8bit):	7.91603970812188
Encrypted:	false
SSDEEP:	3072:bKzwJCcIe4woKmWVlBL2o418Gb0+VRLf0ld0GY3cQ39Vm2I:bKzwjIe41KmWVlNK18Gb0OV8ld0GecQu
MD5:	443C58245EEB233D319ABF7150B99C31
SHA1:	F889CE6302BD8CFBB68EE9A6D8252E58B63E492D
SHA-256:	99CA6947D97DF212E45782BBD5D97BFB42112872E1C42BAB4209CEEDF66DC760
SHA-512:	081F3EE4A5E40FDC8BB6F16F2CFD47EDDE2BD8F3B5349775526092A770B090C05308D4289ECDDA3D541CF7F0579AC64B529930FD128EDAD9B0991DFA00B0E9 BC
Malicious:	false
Preview:	.....#.....:.....`.....a.~...b.....c.k...d.....e.....f.....g.\...h.V...i.....j.....k.o"..l..$..m.//..n..9..o..<..p..@..q.DD..r..F..s..G..t.,K..u..M..v.LO..w..S..x..V.....Y.....[.....\.....^....*_....De.....j .....l....`n.....n.....o.....q.....r.....u.....x.....{.....].....'....M.....K.....I.....Y....\.....&.....#...d*...",....0....4....>...:A...I...vM....W...Na...e....g. ...o...ex...My...z...|.....p.....@.....{.....-.....y.....$.....(.....).U...*.7...+.....,=...-...../.....0.....1.....2.....3.d...4.....5.....6.....7.....8.. ...9.r...;.6...<.....=.....>.....?.[...@.$...A.....B.....C.....D.....G.....o.....d.....[.....K..... .....!.....".X...#.....$.[...%.....&.q..'.....(....*.....+.g...,....-.A..... ./."...0.....1.....2.g...3...

C:\Users\user\AppData\Local\Programs\WolferVPN\chrome_200_percent.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	195935
Entropy (8bit):	7.941514552320428
Encrypted:	false
SSDEEP:	3072:A4DQYaE/N6gbrvy/+JPnKmWVlBafR54x5GMR+F44ffbdZnYw9p4AbIVGYoDd+Hxf:A4DQYaSN6gnvyWnKmWVlSgx5GMRejnbA
MD5:	81B5B74FE16C7C81870F539D5C263397
SHA1:	27526CC2B68A6D2B539BD75317A20C9C5E43C889
SHA-256:	CB4FD141A5C4D188A3ECB203E9D41A3AFCA648724160E212289ADCAC666FBFF4
SHA-512:	B2670E2DFA495CCC7874C21D0413CFBEBFD4A2F14FC0217E823EC6A16AC1181F8E06BFE7C2D32543167BC3A2E929C7F0AF1A5F90182E95913BA2292FA7CADE 80
Malicious:	false
Preview:	.....#.....:.....`.@...a.O...b.3...c.....d.6...e.1...f..%..g.++..h.;...i..5..j..9..k.?B..l..F..m..Z..n.[o..o..t..p..~..q.:...r....s.s...t.....u.....v.....w....x.....r.....l..... .....*.....?.....3.....8.....w.....j.....s.....H....._R...$U....Y....c....e...Th....m....x...az.....l....N.....4....`.....`.....a..... .....3.....n.....E.....!....#%... ,....>/....W6.....=....IA....zh....pi....Pn..(.3s..).at..*.{v..+..w..,Zx..-..y....`{../..|..0.d~..1.....2.....3.d...4.R...5.3...6.....7., ...8.2...9....;.....<.....=.....>.0...?.T...@.u...A.i...B.=...C....D.....G._.....Y.....v.....!....W.....0.....D..... .....!....."....#.....$.....%.?...&.....'.p...(....*.....+.....,.....-.k.... ...../.....0.G...1.....2.E...3...

C:\Users\user\AppData\Local\Programs\WolferVPN\d3dcompiler_47.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4916712
Entropy (8bit):	6.398049523846958
Encrypted:	false
SSDEEP:	49152:KCZnRO4XyM53Rkq4ypQqdoRpmruVNYvkaRwvhiD0N+YEzI4og/RfzHLeHTRhFRNc:xG2QCwmHPnog/pzHAo/A6l
MD5:	2191E768CC2E19009DAD20DC999135A3
SHA1:	F49A46BA0E954E657AAED1C9019A53D194272B6A
SHA-256:	7353F25DC5CF84D09894E3E0461CEF0E56799ADBC617FCE37620CA67240B547D
SHA-512:	5ADCB00162F284C16EC78016D301FC11559DD0A781FFBEFF822DB22EFBED168B11D7E5586EA82388E9503B0C7D3740CF2A08E243877F5319202491C8A641C97
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[3..]...]...]..e\...]...\.5.]..e...]..wX...]..wY...]..e^...]..eX.y.]..eY...]..e]. ..]..eU./.]..e....]..e_...].Rich..]..... PE..d...^.}`..... " .....8.....<).....K.....:FK...`A.....`%G.x....(G.P.....J.@.....H.....J..%.... J.....p.D.p.....S<.(...pR<.@.....S<.(.....text....8.....8..... ..`.rdata...F....8..P....8.....@..@.data...`....@G.....@G.....@....pda ta.....H.....@H.....@..@.rsrc...@.....J.....@J.....@..@.reloc.....J.....PJ.....@..B.....

C:\Users\user\AppData\Local\Programs\WolferVPN\ffmpeg.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2880000
Entropy (8bit):	6.6993392201014155
Encrypted:	false
SSDEEP:	49152:AZ2KxYmwFfgQQs0ShPrF0/zO6R0gRhPj3hTUctrRhuwSnKxqgI5lN8N3lzl3hqzv:Uofp1Pyi54wnKxqg4lNhh9
MD5:	2A7C224800F0A752DB6EAF3AB7CAE796
SHA1:	B718B4B7AE938A10042BCDB2AEC45894E76E21DA
SHA-256:	6D0F59C9E75CA6B16FF63A005045E33E201BFF2F9D4900B9256CF2F7032722D5
SHA-512:	D2301BBBBE3E882D34BDCA48A3B9C89AE8457A38000AFC9B8B23EC797FA50642316E33C79DBE9F1954BAC39F66531D9792C65D02524E444E3B7B7FE4E49CF8DB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...I.Ke..... " ..... ". ..... B.....`A.... .....*.....*.(.....@.....A..4....).....).(....#.@.....H.*.P.....text....."....."..... ..`.rdata.....#.....#..... @..@.data.....*.."....*.....@....pdata.....@.....*.....@..@.00cfg..8....pA.....+.....@..@.gxfg....,....A.....+.....@..@.retplne.....A.....+.....tls.. .....A.....+.....@..._RDATA..\....A.....+.....@..@.reloc...4....A..6....+.....@..B.....

C:\Users\user\AppData\Local\Programs\WolferVPN\icudtl.dat

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	10544880
Entropy (8bit):	6.276833777601164
Encrypted:	false
SSDEEP:	98304:GKPBQYOo+ddlymOk25flQCUliXUxiG9Ha93Whla6ZGdnp/8j:GKPBhORjOhCliXUxiG9Ha93Whla6ZGr4
MD5:	2134E5DBC46FB1C46EAC0FE1AF710EC3
SHA1:	DBECF2D193AE575ABA4217194D4136BD9291D4DB
SHA-256:	EE3C8883EFFD90EDFB0FF5B758C560CBCA25D1598FCB55B80EF67E990DD19D41
SHA-512:	B9B50614D9BAEBF6378E5164D70BE7FE7EF3051CFFF38733FE3C7448C5DE292754BBBB8DA833E26115A185945BE419BE8DD1030FC230ED69F388479853BC0FCB
Malicious:	false
Preview:	...'.....CmnD..... Copyright (C) 2016 and later: Unicode, Inc. and others. License & terms of use: http://www.unicode.org/copyright.html .Q....B.....B...#...B.. $...B..p$.. .B...$...B...%...B..`P...C...P...C...Q..(C.....<C.....OC.....bC..@...uC.....C..P....C.....C.....C..p....C.. ....C.....C.....D..p... D.....3D..0...FD.....YD.....ID.....D.....D..0....D... ....D..p....D.....D..@....D.....E.....E..@...*E.....=E..P...NE.....bE.....rE..@....E.....E.....E..P....E.....E.....E..@....F.....F.....'F..0...7F..P...JF.....aF.....qF...G...F.. H...F. .`K...F...K...F...L...F...-...F...c...G....'.'G....'.>G..@.'.UG..0.'.oG....'..G...!'..G...!'..G..P&'..G...)'..G..@*'..H..`.(..H...e).7H..0.).VH...)*.xH....*..H....*..H...P+..H...Y+..H...Z+..I...]+. I. .`^+.9I.. .+.UI....+.II....+..I..P.-..I...=...I.....I.....I.. ....J..p....J.....-J..p...EJ.....ZJ.....rJ..`....J..@....J.....J.....J..0....J.....J.....J..0....K..@....K..../.2K.../.GK..../.\K..

C:\Users\user\AppData\Local\Programs\WolferVPN\libEGL.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	480256
Entropy (8bit):	6.336558815218672
Encrypted:	false
SSDEEP:	6144:s4itlpEJVqKqK5Z5UibKsBHI0Sfnx+lXGpeOQHA93Gb3sm:s4itlpAqKqK5Z5U+jBolfnjIyG
MD5:	45EF2DF5F6AAF1BA9ECDDBFA0F07574C
SHA1:	0F93C5B9775AD32D342963F4DD27BB0CDAADD793
SHA-256:	22BA0C9ACF55F4FA5DF7098B70D020D65619703A282D45B288632F248CD23B4E
SHA-512:	99423F92EEDA8E907D0E2C0A2A7DA5A89E64B7B4B4D5F93EE48C91C9F2A0D415377B373FA656386F1FC0D6C8556E57CE2D4001650A47F5F6F4D5CA217D5FADBB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse

Preview:	MZx....................@.................................x...........!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke.........." ....`A.... ..................................P"......f0..(.......x........B.............................................(...@1..@...........3..............................text...]....... ................. ..`.rdata..D....0.......$............. @..@.data....K.........................@....pdata...B.......D.................@..@.00cfg..8....`....................@..@.gxfg...`$...p...&................@..@.retplne............:..................tls....!....... .....<.............@..._RDATA..\...........>.............@..@.rsrc...x...........@.............@..@.reloc..............F.............@..B... ....

C:\Users\user\AppData\Local\Programs\WolferVPN\libGLESv2.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7418880
Entropy (8bit):	6.464871257930227
Encrypted:	false
SSDEEP:	49152:x2b3imtb1uWsvZRUCXQNMBbGUa/XFfOpvQnDwX+xjA7LAlgRg37Qil+id3pFJs7y:x7RWft4NV+sduHox6gWE5lHoFX
MD5:	0BC536DDA0CC8195F58A48B9500E3D48
SHA1:	D1FD4FFA994B497FF927C2851660E929F3079AEF
SHA-256:	4E7AFC3A650CF414DEBA33AB4D755F601624A8E24934B43A958ECA933D65D8EA
SHA-512:	372B5E9890EDA267097DD92ACD407D422C3621452C19720C510C44A3D468779D12D5A3D557C2CA64F0BB86C6766665E2BC100CA465FCF604DF2ED950F406A63
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZx....................@.................................x...........!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke.........." .....hV...........J.....................................@r....... ....`A..........................................h.......i.d....Pq.......n.TR..........`q.....\=h....................0<h.(.....V.@............i..... .h.@...................text...egV......hV................ ..`.rdata..L.....V. .....lV............@..@.data........pj......Pj............@....pdata..TR....n..T....m............@..@.00cfg..8.....p......(p............@..@.gxfg....+....p..,...*p............@..@.retplne..... q......Vp... ....tls....:....0q......Xp............@..._RDATA..\....@q......Zp............@..@.rsrc........Pq......\p............@..@.reloc.......`q......bp............@..B... ....

C:\Users\user\AppData\Local\Programs\WolferVPN\resources.pak

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\WolferVPN.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>5193850</td></tr>
<tr><td>Entropy (8bit):</td><td>7.9952704707488165</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>98304:qg1zetaMcKWPxgWMp1W/ywNAWsh11fHcMtyrwr+oxPf0yO1WODHxSkLyz7ai6y:qgVetWxWF1pkshH8M4krFPf0FIG27sy</td></tr>
<tr><td>MD5:</td><td>043DBE3EAF0BDE424185A3843E321F83</td></tr>
<tr><td>SHA1:</td><td>580AC5FDE14E6D177D6F45D2E40D435CC7EDC8D0</td></tr>
<tr><td>SHA-256:</td><td>0C967CB604D5066F1AB609E81895C1271475A2E1B4B3D5930EEA720FC218781B</td></tr>
<tr><td>SHA-512:</td><td>44814AAEC681922594528D0ED1A4D2E935045220D09E065647B53455931EAEB3B737C87032B611D7EAD621379AE653A9C5D6D87C828C1961C54129124234EBC3</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>............f........).....+....b/...8.A...8.J...8.M...8.`...8-i...8Hp...8.r...8-y...8.{...80}...8s....8e....8.....8.....8....8+....8W....8)....8....8.....8|....8.....8;....8H....8.....8.....8y....8o....8z....8 .....8.....8^....8.....9.....9.....9.....99....9.....9.....9\"...9.B...9kD...9.I...9.S...9.U...9.V...9|W...9.Z...9.Z...9R[...9.`...9.f...9.w...9.....9x....9.....@.....@.....@....@.....@.....@.....@... ..@`....@&....@.....@.....@.....@....8E....9EB...:EV...;E....<E."..=Eu-..>E....?E./..@E.0..AEQH..BEL....FSD...F.G...U4....UH....U/....U.....U.....U....U.....U5....U.....U.....U.... .U.....U6....U.....U.....U.....U.....U.....U.....U.....VM....V^....V.....V.!...V.+...VJ2...V0A...V.D...V.J...Vi]...V.e...V.j...VK~...V....V.....Vn..."V....#Ve...$V,...%V....&V....'V(...(V... .)V....*V>...+V@....W.....WUP...W}T.....V.....Y..........C.....y..........y.....j...........6N.....V....L^....Rc....$e....Dj.....o....1w.............................-........../....0.....2.....3.....4.....5.4.</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\WolferVPN\snapshot_blob.bin

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	259202
Entropy (8bit):	4.177720672914121
Encrypted:	false
SSDEEP:	1536:N8eVec2PhNMqkPhmplLx3FtscrrDKrVTT9gXA4SuoveydoBaDEtu/wMHOdxpMKrF:76N6PkplLxHscrXeQZb0G0mvY6T
MD5:	3A4095538E021B84396B3CE25AFFAFC3
SHA1:	CFC20771227B3C1F3197FF6A91CEE68555AFB247
SHA-256:	C1C9145735032BFF20B2FFF50A4B92AE9CF47290F433E3F3B32E3B232D610C59
SHA-512:	7B71083180F237F5F37CBE7A9755F6606708B959986562F9C5880CCCEA17B80A5187649FC0CB6965A8B40526BCB2CB6D980D364BE528465290658B4D9084348E
Malicious:	false
Preview:	.........J.&11.4.183.29-electron.0...h...B%...Y..........a........a........a........ar.......a........a.............].D.......M....`$.......m.D.......=....`$.......D.......M....`$. ......u.D.......M....`$.........D.......A....`D.........D.......M....`$.......M.D.......M....`$.......D.......M....`$.......D.!.....M....`$.......q.D.%.....E....`$.......D.).....M....`$......ID.-.....M....`$... ....D.1.....M....`$.......D.5.....M....`$....(Jb...(L.....@..F^......`.....(Jb...,P.....@..F^..`.....H...IDa........Db............D`.......D`.....D]D....D`......Wla..........Wla..........Wla..........Wla.... ....Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla...........Wla............L............... ....

C:\Users\user\AppData\Local\Programs\WolferVPN\v8_context_snapshot.bin

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	578034
Entropy (8bit):	5.245532016724801
Encrypted:	false
SSDEEP:	6144:alKQ1+Ku6X5O8QgZbNg8zvEjbwTBH32jezyjPX:aV1oeLvs4mCG
MD5:	5DB8A5BB87C7999343F30128979057A1
SHA1:	C4177C2FE973A495DB59B6228AC26264EEC46A4D
SHA-256:	5B1F69F39F3D5865DCE13EE3BDBC1AF2938F5CC4C056DC9F9E213E9AF346AD4B
SHA-512:	DA2D516251376952729A33DE2CD23764290D400FAFC49642F2CCD799E3F989CCE4D5561A76D380A950B77B53B50148DEC9089C30DE6C3DC38666237E196E569
Malicious:	false
Preview:	..... .R.11.4.183.29-electron.0.....p.....*....y.....@p..a.....a.....aT.....ar.....a.....a.....].D.....M....`$.....m.D.....=....`$.....D.....M ....`$.....u.D.....M....`$.....D.....A....`D.....D.....M....`$.....M.D.....M....`$.....D.....M....`$.....D.!....M....`$.....q.D.%....E....`$.....D.)....M....`$.....ID.-.....M....`$..... .D.1.....M....`$.....D.5....M....`$....(Jb...(L.....@..F^.....`.....(Jb...,P.....@..F^..`.....H...IDa.....Db.....D`.....D`.....D]D....D`.....Wla.....Wla.....Wla.....Wla..... ....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....L..... .....

C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5251072
Entropy (8bit):	6.341324832913826
Encrypted:	false
SSDEEP:	49152:Ab03fn3GIdr1DO1N8jvfWSrvOuyEE0+w7rz77gpxbhk0H4t38mvttDpSHUoeygs4:d3v3xDvRTGVgt38mvt1pSH0adU
MD5:	516C5B93B1C13AF0AD393BFF6AA4E259
SHA1:	A8823263EE4C2B7CED5AEA055E6F4105DF09E478
SHA-256:	2377FD655C1E0B6275F109258F3AF70161996F6CCBF8D67BB654D3A9EDF6D5B9
SHA-512:	B976C2373525DD1AC9493D281EC5A1685D1C63B41C44DB6F0DF10915A6C97A2E041D3F00485AADF7B52695C901D5AB1FE2FFE0CAA7AEEAE6874065B185D81A 22
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke.....".....?..z.....9.....Q.....`A.... .....zK.~...f.K.P.....Q.....@O._..... Q.h}...8K.....7K.(...@.?.@.....K.P.....text.....?.....?..... ..`.rdata.....?.....?... .....@..@.data.....L.....pL.....@....pdata..._...@O..`....N.....@..@.00cfg..8.....P.....fO.....@..@.gxfg.....,....P.....hO.....@..@.retplne.....P.....O... .....tls....Q.....P.....O.....@...._RDATA..\.....Q.....O.....@..@.rsrc.....Q.....O.....@..@.reloc..h}... Q..~....O.....@..B..... .....

C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	4.724752649036734
Encrypted:	false
SSDEEP:	3:YD96WyV18tzsmyXLVi1rTVWSCwW2TJHzeZ18rY:Y8WyV18tAZLVmCwXFiZ18rY
MD5:	8642DD3A87E2DE6E991FAE08458E302B
SHA1:	9C06735C31CEC00600FD763A92F8112D085BD12A
SHA-256:	32D83FF113FEF532A9F97E0D2831F8656628AB1C99E9060F0332B1532839AFD9
SHA-512:	F5D37D1B45B006161E4CEFEEBBA1E33AF879A3A51D16EE3FF8C3968C0C36BBAFAE379BF9124C13310B77774C9CBB4FA53114E83F5B48B5314132736E5BB449 6F
Malicious:	false
Preview:	{"file_format_version": "1.0.0", "ICD": {"library_path": ".\\vk_swiftshader.dll", "api_version": "1.0.5"}}

C:\Users\user\AppData\Local\Programs\WolferVPN\vulkan-1.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped

Size (bytes):	931840
Entropy (8bit):	6.56671155058839
Encrypted:	false
SSDEEP:	24576:FoHDVVdrfQ09CPKuy0O0Q6Z5W0DYsHA6g3P0zAk7m+:FuVdrl0GKuy066Z5W0DYsHA6g3P0zAk5
MD5:	D1F1609B93993A1C74872FAF7694B01D
SHA1:	4237815549B77F3509EE99F8ED6A86DE6C15AA20
SHA-256:	D0615DC92873F5FC92A74CDED1E0EC34A702D6A3E671778C841BE20DA2CD4549
SHA-512:	CD80B50476C4358E06736789B99C5F8C97F3FA5C7DEE85610EED26A5EA42189F6475F97FF00B7D11C15DBE72B9B7734EB01732275A1B510D13663DC775EFF81
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke....." .....x.....`A.... .....0...<!..l...P.....o.....L...<..... ...(...@...@.....text....v.....x..... ..`.rdata.....\|..... @..@.data....L..... ...d.....@....pdata...o.....p.....@..@.00cfg..8....@.....@..@.gxfg...P(...P...*.....@..@.retplne..... .....tls.. ....."....."....@..._RDATA..\.....$.....@..@.rsrc.....&.....@..@.reloc..L.....*.....@..B..... .....

C:\Users\user\AppData\Local\Temp\8aa2ec43-5e03-40f0-b44b-d7dcf4df059c.tmp.node

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1648128
Entropy (8bit):	6.563147955168653
Encrypted:	false
SSDEEP:	24576:tUgSe+M9LbxN3FbrbcP8w40RBvle2M0BsbHO9wn0eRu2vL/qDi/jZHFf:T+M9B08Mvle2fBsRD
MD5:	22587652E488CAE64A03C8038A44A259
SHA1:	9359EECF5F15A97C5ADE7B1086B5B5097928AA2E
SHA-256:	5AC0D196837E9C6E7CD779235AB4F45738DFD25178FE58EF4DAF66AB5705F356
SHA-512:	C590CF0FD56A3CB68DB65DD973AAF76972A6F44658B1E2FD0FA60E12DC69F76199A3794460694A3C4FF9D370CC99BF4134AC1A43B99CDEFD7EE4D66584F4D0 C9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[a....xY..xY..xY.r{X..xY.r}X..xY.r|X=.xYMu|X..xYMu{X..xYMu}X6. xY.ryX..xY..yY..xY.uqX..xY.uxX..xY.u.Y..xY.uzX..xYRich..xY.....PE..d....bLe....." .....4.....`.....`...P... (....`.....`.....p.....p.....).8.....P.....@.....text....3.....4..... ..`.rdata.....P.....8.....@..@.data...`h.....R.....@....p data.....`....."....."....@..@_RDATA.....P.....@..@.rsrc.....`.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\b1c3f10e-540e-46f8-9bee-83879b20c9f6.tmp.node

Process:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	152576
Entropy (8bit):	6.214761833394253
Encrypted:	false
SSDEEP:	3072:Bi9h7qgZQj5hsmCi1REPUuxHi8r2qlakV1lKaea:BiDqes5hYiwPlxHiopK3
MD5:	A24B00648797927AF983B1736F53C258
SHA1:	5FB4F066C89E6F7F4E185E9D908F48AEA88832EA
SHA-256:	1ABF0289710A7B8A886653CCE8BD7D69D869074809E8A9AC8926070BA16888EE
SHA-512:	19A3A868BA7E1DDF96FF4C8FC1E35D9948DBA5D92A7F819DDC75D2A6A0068CD5E6DFA272009AD3880D11AB357CCE4238CFBB4C21CECFDC78CE8063850334 CF4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41% • Antivirus: Virustotal, Detection: 40%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t..~'..~'..~'/.}&..~'/.{&v.~'/.z&..~'X.z&.~'X.}&..~'X.{&.~'/..&..~'.. .'..~'..w&..~'..'..~'..\|&..~'Rich..~'.....PE..d.....Ve....." ...$.j.....` .....-..<.....`..... ...p..... .....`...@.....$..@.....text....j.....j..... ..`.rdata..B.....n.....@..@.data.....@.....&.....@....pdata.....`.....2.....@..@_ RDATA..\.....H.....@..@.rsrc.....J.....@..@.reloc.....L.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\LICENSE.electron.txt

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	ASCII text

Category:	dropped
Size (bytes):	1096
Entropy (8bit):	5.13006727705212
Encrypted:	false
SSDEEP:	24:36DiJHxRHuyPP3GtIHw1Gg9QH+sUW8Ok4F+d1o36qjFD:36DiJzfPvGt7ICQH+sfIte36AFD
MD5:	4D42118D35941E0F664DDDBD83F633C5
SHA1:	2B21EC5F20FE961D15F2B58EFB1368E66D202E5C
SHA-256:	5154E165BD6C2CC0CFBCD8916498C7ABAB0497923BAFCD5CB07673FE8480087D
SHA-512:	3FFBBA2E4CD689F362378F6B0F6060571F57E228D3755BDD308283BE6CBBEF8C2E84BEB5FCF73E0C3C81CD944D01EE3FCF141733C4D8B3B0162E543E0B9F3E63
Malicious:	false
Preview:	Copyright (c) Electron contributors.Copyright (c) 2013-2020 GitHub Inc...Permission is hereby granted, free of charge, to any person obtaining.a copy of this software and associated documentation files (the."Software"), to deal in the Software without restriction, including.without limitation the rights to use, copy, modify, merge, publish,.distribute, sublicense, and/or sell copies of the Software, and to.permit persons to whom the Software is furnished to do so, subject to.the following conditions:..The above copyright notice and this permission notice shall be.included in all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,.EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF.MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND.NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE.LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION.OF CONTRACT, TORT OR OTHERWISE, ARISIN

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\LICENSES.chromium.html

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	8245721
Entropy (8bit):	4.70761969468716
Encrypted:	false
SSDEEP:	24576:dbTj6ck6f5kVWS6RqLsWN3Omfpe666A6f6X6TTHW9GqpaE:tEx/i
MD5:	0E3E4362F785AFF0B9E1852B1064C0F1
SHA1:	A42CCB51E72BDCB5BB905A62EFAA28857DEF3A17
SHA-256:	BD3EE49A5AB19D15DDC44B421B0BDEFCE587790786989AE77CF3DDF1E6A2BA8D
SHA-512:	193B57EFC5F5971FBD9E4EA1A80B34AADCC2A814FF49C4C06AFE972BF327E98FF0498217A8BDEF984B10FDEC6E7858A6FB88C0B14936E0C6B404387A426B87F2
Malicious:	false
Preview:	Generated by licenses.py; do not edit. --><!doctype html>.<html>.<head>.<meta charset="utf-8">.<meta name="viewport" content="width=device-width">.<meta name="color-scheme" content="light dark">.<title>Credits</title>.<link rel="stylesheet" href="chrome://resources/css/text_defaults.css">.<link rel="stylesheet" href="chrome://credits/credits.css">.</head>.<body>.Credits.Print. Chromium <3s the following projects -->. .2-dim General Purpose FFT (Fast Fourier/Cosine/Sine Transform) Package.homepage.<input type="checkbox" hidden id="0">.<label class="show" for="0" tabindex="0"></label>. .<pre>Copyright(C) 1997,2001 Takuya OOURA (email: ooura@kurims.kyoto-u.ac.jp)..You may us

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\WolferVPN.exe

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	163343360
Entropy (8bit):	6.732960636432368
Encrypted:	false
SSDEEP:	1572864:VOehMi9HmQapOF/wcuOG/KTlWoqYtUMogmhQXoqAfIgrWAdBb9pTHPe3HdYYGQc1:4ZK9PUddCvs
MD5:	4AD8066DFB8E65195E5733DDFD8A1AC7
SHA1:	8225752BBC6C6720F92B8890117A76576AB5D951
SHA-256:	BB3651F02D8CDBC962EC910EC5E6DE3BAD9DD94CBB811DA098116E19C4BE7C0F
SHA-512:	BA5951A9455A06060AA349F66D2AF97227E5617B2D6867CA3AB0AA1082D3528D0AE43481F0C8FFD489A84B748CCCC88FE5AAD805F753E339B691F836B2905C5D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...I.Ke.....".....f.....j%.....@.....`.....[..'...^.h.....'A.....L..p.Q.....PzQ.(... ...@.....^.`....@[.....text..... ..`.rdata....n.....n.....@..@.data.....C...b.....b.....@....pdata...'A.....(A...j.....@..@.00cfg..0.....@..@.gxfg...pA.....B.....@..@.retplne..... .....rodata.....0..... ..... ..`.tls.....P.....2.....@...CPADinfo8....`.....8.....@...LZMADEC.....p.....:..... ..`_RDATA..\.....L.....@..@malloc_h..... .N..... ..`.rsrc.....P.....@..@.reloc...L.....N.....@..B.....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\chrome_100_percent.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data

Category:	dropped
Size (bytes):	135956
Entropy (8bit):	7.91603970812188
Encrypted:	false
SSDEEP:	3072:bKzwJCcIe4woKmWVlBL2o418Gb0+VRLf0ld0GY3cQ39Vm2l:bKzwjIe41KmWVlNK18Gb0OV8ld0GecQu
MD5:	443C58245EEB233D319ABF7150B99C31
SHA1:	F889CE6302BD8CFBB68EE9A6D8252E58B63E492D
SHA-256:	99CA6947D97DF212E45782BBD5D97BFB42112872E1C42BAB4209CEEDF66DC760
SHA-512:	081F3EE4A5E40FDC8BB6F16F2CFD47EDDE2BD8F3B5349775526092A770B090C05308D4289ECDDA3D541CF7F0579AC64B529930FD128EDAD9B0991DFA00B0E9BC
Malicious:	false
Preview:	.....#.....:.....`.....a.~...b.....c.k...d.....e.....f.....g.\...h.V...i.....j.....k.o"..l..$..m.//..n..9..o..<..p..@..q.DD..r..F..s..G..t.,K..u..M..v.LO..w..S..x..V.....Y.....[.....\.....^....*_....De.....j.....l....`n.....n.....o.....q.....r.....u.....x.....{.....'....M.....K.....I.....Y....\.....&.....#...d*...",....0....4....>...:A...I...vM....W...Na...e....g.....o...ex...My...z...\|.....p.....@.....{.....-.....y.....$.....(.....).U...*.7...+.....,=...-...../.....0.....1.....2.....3.d...4.....5.....6.....7.....8..9.r...;.6...<.....=.....>.....?.[...@.$...A.....B.....C.....D.....G.....o.....d.....[.....K..... .....!....".X...#.....$.[...%.....&.q..'.....(....*.....+.g...,....-.A......./."...0.....1.....2.g...3...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\chrome_200_percent.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	195935
Entropy (8bit):	7.941514552320428
Encrypted:	false
SSDEEP:	3072:A4DQYaE/N6gbrvy/+JPnKmWVlBafR54x5GMR+F44ffbdZnYw9p4AbIVGYoDd+Hxf:A4DQYaSN6gnvyWnKmWVlSgx5GMRejnbA
MD5:	81B5B74FE16C7C81870F539D5C263397
SHA1:	27526CC2B68A6D2B539BD75317A20C9C5E43C889
SHA-256:	CB4FD141A5C4D188A3ECB203E9D41A3AFCA648724160E212289ADCAC666FBFF4
SHA-512:	B2670E2DFA495CCC7874C21D0413CFBEBFD4A2F14FC0217E823EC6A16AC1181F8E06BFE7C2D32543167BC3A2E929C7F0AF1A5F90182E95913BA2292FA7CADE80
Malicious:	false
Preview:	.....#.....:.....`.@...a.O...b.3...c.....d.6...e.1...f..%..g.++..h.;...i..5..j..9..k.?B..l..F..m..Z..n.[o..o..t..p..~..q.:...r....s.s...t.....u.....v.....w....x.....r.....l.....*.....?.....3.....8.....w.....j.....s.....H...._R...$U....Y....c....e...Th....m....x...az.....l....N.....4....`.....`.....a.....3.....n.....E.....!....#%.... ,....>/....W6.....=....IA....zh....pi....Pn..(.3s..).at..*.{v..+..w..,.Zx..-..y....`{../..\|..0.d~..1.....2.....3.d...4.R...5.3...6.....7.,...8.2...9....;.....<.....=.....>.0...?.T...@.u...A.i...B.=...C....D.....G._.....Y.....v.....!.....W.....0.....D..... .....!....."....#.....$.....%.?...&.....'.p...(.....*.....+.....,.....-.k......./.....0.G...1.....2.E...3...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\d3dcompiler_47.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4916712
Entropy (8bit):	6.398049523846958
Encrypted:	false
SSDEEP:	49152:KCZnRO4XyM53Rkq4ypQqdoRpmruVNYvkaRwvhiD0N+YEzl4og/RfzHLeHTRhFRNc:xG2QCwmHPnog/pzHAo/A6l
MD5:	2191E768CC2E19009DAD20DC999135A3
SHA1:	F49A46BA0E954E657AAED1C9019A53D194272B6A
SHA-256:	7353F25DC5CF84D09894E3E0461CEF0E56799ADBC617FCE37620CA67240B547D
SHA-512:	5ADCB00162F284C16EC78016D301FC11559DD0A781FFBEFF822DB22EFBED168B11D7E5586EA82388E9503B0C7D3740CF2A08E243877F5319202491C8A641C97
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|3..]....]...]..e\...]...\.5.]..e...]..wX...]..wY....]..e^...]..eX.y.]..eY...]..e]...]..eU./.]..e....]..e_...].Rich..]..... .....PE..d...^.}`..... " .....8.....<).....K.....:FK...`A.....`%G.x....(G.P.....J.@.....H.....J..%....J.....p.D.p.....S<.(...pR<.@.....S<.(.....text....8.....8..... ..`.rdata...F....8..P....8.....@..@.data...`....@G.....@G.....@....pdata.....H.....@H.....@..@.rsrc...@.....J.....@J.....@..@.reloc.....J.....PJ.....@..B.....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\ffmpeg.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2880000
Entropy (8bit):	6.6993392201014155

Encrypted:	false
SSDEEP:	49152:AZ2KxYmwFfgQQs0ShPrF0/zO6R0gRhPj3hTUctrRhuwSnKxqgI5IN8N3lzl3hqzv:Uofp1Pyi54wnKxqg4INhh9
MD5:	2A7C224800F0A752DB6EAF3AB7CAE796
SHA1:	B718B4B7AE938A10042BCDB2AEC45894E76E21DA
SHA-256:	6D0F59C9E75CA6B16FF63A005045E33E201BFF2F9D4900B9256CF2F7032722D5
SHA-512:	D2301BBBBE3E882D34BDCA48A3B9C89AE8457A38000AFC9B8B23EC797FA50642316E33C79DBE9F1954BAC39F66531D9792C65D02524E444E3B7B7FE4E49CF8DB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke....." ....."..... B.....`A.... .....*.....*.(.....@.....A..4....).....).(...."#.@.....H.*.P.....text....."....."..... ..`.rdata.....#.....#..... @..@.data.....*..".....*.....@....pdata.....@.....*.....@..@.00cfg..8....pA.....+.....@..@.gxfg.....A.....+.....@..@.retplne.....A.....+.....tls.. .....A.....+.....@..._RDATA..\.....A.....+.....@..@.reloc...4....A..6....+.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\icudtl.dat	
Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	10544880
Entropy (8bit):	6.276833777601164
Encrypted:	false
SSDEEP:	98304:GKPBQYOo+ddlymOk25flQCUliXUxiG9Ha93Whla6ZGdnp/8j:GKPBhORjOhCliXUxiG9Ha93Whla6ZGr4
MD5:	2134E5DBC46FB1C46EAC0FE1AF710EC3
SHA1:	DBECF2D193AE575ABA4217194D4136BD9291D4DB
SHA-256:	EE3C8883EFFD90EDFB0FF5B758C560CBCA25D1598FCB55B80EF67E990DD19D41
SHA-512:	B9B50614D9BAEBF6378E5164D70BE7FE7EF3051CFFF38733FE3C7448C5DE292754BBBB8DA833E26115A185945BE419BE8DD1030FC230ED69F388479853BC0FCB
Malicious:	false
Preview:	...'.....CmnD..... Copyright (C) 2016 and later: Unicode, Inc. and others. License & terms of use: http://www.unicode.org/copyright.html .Q....B.....B...#...B.. $...B..p$.. .B...$...B...%...B..`P...C...P...C...Q..(C.....<C.....OC.....bC..@...uC.....C..P....C.....C.....C..p....C.. ....C.....C.....D..p... D.....3D..0...FD.....YD.....ID.....D.....D..0....D... ....D..p....D.....D..@....D.....E.....E..@...*E.....=E..P...NE.....bE.....rE..@....E.....E.....E..P....E.....E.....E..@....F.....F....'F..0...7F..P...JF.....aF.....qF...G...F.. H...F. .`K...F...K...F...L...F...-...F...c...G....'.'G....'.>G..@.'.UG..0.'.oG....'..G...!'..G...!'..G..P&'..G...)'..G..@*'..H..`.(..H...e).7H..0.).VH...)*.xH....*..H....*..H...P+..H...Y+..H...Z+..I...]+. I. .`^+.9I.. .+.UI....+.II....+..I..P.-..I...=...I.....I.....I.. ....J..p....J.....-J..p...EJ.....ZJ.....rJ..`....J..@....J.....J.....J..0....J.....J.....J..0....K..@....K..../.2K.../.GK..../.\K..

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\libEGL.dll	
Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	480256
Entropy (8bit):	6.336558815218672
Encrypted:	false
SSDEEP:	6144:s4itlpEJVqKqK5Z5UibKsBHI0Sfnx+lXGpeOQHA93Gb3sm:s4itlpAqKqK5Z5U+jBolfnjIyG
MD5:	45EF2DF5F6AAF1BA9ECDDBFA0F07574C
SHA1:	0F93C5B9775AD32D342963F4DD27BB0CDAADD793
SHA-256:	22BA0C9ACF55F4FA5DF7098B70D020D65619703A282D45B288632F248CD23B4E
SHA-512:	99423F92EEDA8E907D0E2C0A2A7DA5A89E64B7B4B4D5F93EE48C91C9F2A0D415377B373FA656386F1FC0D6C8556E57CE2D4001650A47F5F6F4D5CA217D5FADBB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke....." ....`A.... .....P"......f0..(.....x.....B.....(...@1..@.....3.....text...]..... ..... ..`.rdata..D....0.....$..... @..@.data....K.....@....pdata...B.....D.....@..@.00cfg..8....`.....@..@.gxfg...`$...p...&.....@..@.retplne.....:.....tls....!..... .....<.....@..._RDATA..\.....>.....@..@.rsrc...x.....@.....@..@.reloc.....F.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\libGLESv2.dll	
Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7418880
Entropy (8bit):	6.464871257930227
Encrypted:	false

SSDEEP:	49152:x2b3imtb1uWsvZRUCXQNMBbGUa/XFfOpvQnDwX+xjA7LAIgRg37QiI+id3pFJs7y:x7RWft4NV+sduHox6gWE5lHoFX
MD5:	0BC536DDA0CC8195F58A48B9500E3D48
SHA1:	D1FD4FFA994B497FF927C2851660E929F3079AEF
SHA-256:	4E7AFC3A650CF414DEBA33AB4D755F601624A8E24934B43A958ECA933D65D8EA
SHA-512:	372B5E9890EDA267097DD92ACD407D422C3621452C19720C510C44A3D468779D12D5A3D557C2CA64F0BB86C6766665E2BC100CA465FCF604DF2ED950F406A63
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke....." .....hV.....J.....@r..... ....`A.....h.....i.d....Pq.....n.TR.....`q.....\=h.....0<h.(.....V.@.....i..... .h.@.....text...egV.....hV..... ..`.rdata..L.....V. .....IV.....@..@.data.....pj.....Pj.....@....pdata..TR....n..T....m.....@..@.00cfg..8.....p.....(p.....@..@.gxfg....+....p.,....*p.....@..@.retplne..... q.....Vp... .....tls....:....0q.....Xp.....@..._RDATA..\....@q.....Zp.....@..@.rsrc.....Pq.....\p.....@..@.reloc.....`q.....bp.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\af.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	390307
Entropy (8bit):	5.42897416012883
Encrypted:	false
SSDEEP:	6144:qu8SyRtgbfbjR985DhdxQ+ICGSBsjA636Zi2Jynq4UtUKnpgmhqxox7sfxSC2C8l:Ry0zbjREda+ICTsjA636Zi2Jynq4UtBz
MD5:	B293CC5EA7DB02649BD7D386B8FA0624
SHA1:	32169B9D009B7A0FB7ECDAF650C989E956291772
SHA-256:	7BB75ADEF02D28819F1BD3B42FA46ED56D6DFBEAE072341997B09B8C1F52D8DC
SHA-512:	496BC72E7B798D02E453EB96D20566B91405BAB774521527EF882C1FCB58F25E2D0718013DDC0D23F7FAD883F4CDE93B57C6CAAEBA8CD18A09665C9F6245F57
Malicious:	false
Preview:	.....=.h.N...i.V...j.b...k.q...l.|...n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}....."....*.....1.....8.....?.....@.....A.....F.....s..... .....G.....Z.....z.....,.....2.....<.....J.....Z.....h.....%.....@.....X.....q..... .....6.....F.....V.....r.....$.....7.....E....._.....t.....6.....j.....r..... ....."....&.....5.....M.....b.....%..... .7..."D...%.j...(.....*.....+.....,...../.....0.....1.#...3./...4.Q...5.I...6.....7.....8.....9.....<.....=.....>.....?.....@.-...A.^...C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\am.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	634666
Entropy (8bit):	4.90303732149975
Encrypted:	false
SSDEEP:	12288:ihHb86uYwT8xiT1XF/gpwozFQd529+lV5ru4yPpx30jH8+A:MbIT8xCXFopwozFQd529+lV5nyPN
MD5:	4CB4B30911E9FBFE6C1DE688CCA821AB
SHA1:	58CC2D8E954B5C74A902F13C522D1F6836769623
SHA-256:	685ECDFF01D4AE92BE1D900EF00FD8632616BC41F18A56E682528F312D4A5167
SHA-512:	6629AF841C52463C46DBEB03E3B4B1CAD550C2DB790C75365D63512E039B3369CDD9F18316E9C50DCF3AA77AA4D2BECB6A87570F3B538B456AF3041D6039344
Malicious:	false
Preview:	.....$.%.h.~...i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z. ...|.&...}.8.....@.....E.....M.....U.....]....d.....k.....r.....s.....t.....y.....0.....Z.....m..... u.....#.....G.....S.....*.....=.....m.....N.....r.....~.....2.....K.....*.....0.....8... ..?.....K.....^.....q.....#.....<.....x.....2.....N.....g.....E.....e.....]..... .....)....l.....y.....*.....g.....1... .l..".n...%.....(.....*.....+.....,".....3.../.U...0.o...1.....3.....4.....5.S...6.....7.....8.....9./...;.K...<.\...=.s. ..>.....?.....@.....A.....C.U.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ar.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	696385
Entropy (8bit):	4.9097761802335675
Encrypted:	false
SSDEEP:	12288:DpJ+LHvZtD9JAO08vYU3X1Y9kbMf5MNi/+det13zMgSENR5:tMqta45F+K
MD5:	7294148BA219909A4909613381EA45AC
SHA1:	A8A70E589760B5EAEAE1A95FE51723CCE48FCA87

SHA-256:	ACC1B352EA206C25AFE88A614346B468F4F78BF23F886883A38DAE905D121DC0
SHA-512:	CABF320E827067EF8EFB7C021FF098430054D125FB50540C06D12167C7D1C6D08449E6A1B33FA4A092CE6C81A600415711005E100B1B756A199E05CA18DBF3B7
Malicious:	false
Preview:	.....].h.....i.....j.%...k.4...l.?...n.G...o.L...p.Y...r._...s.p...t.y...v.....w.....y.....z.....|.....}.....l....b.....'.....M..... .....0.....P.....g.....4.....O.....o.....2.....<.....M.....W.....*.....U..... ....7.....k.....{.....1.....?.....B.....]....|.....(.....v.....-.....8.....\.....y..... .....\.....~.....%.....:.....\.....m... .....".....%.....(.....*.m...+.p...../.....0.....1.!...3.6...4.]...5.....6.....7.....8.=...9.V...;.q...<.....=.....>.....?.....@.....A.....C. %...D.8...E.y...F...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\bg.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	723752
Entropy (8bit):	4.668436211737206
Encrypted:	false
SSDEEP:	12288:L83VytDqWwQkDmLlYMdAs1aQUtjtaVVnFH2mFxadnra35rKN3yoSiVD1BbCeSKnd:LoytDq/DllYMdAs1aQUVGCa35rKsoSiF
MD5:	080CFFA1D4032B7D4BFA217AA00C4F47
SHA1:	525CF2BAF62EC4C90E3A1D89CCE37C9F433C61E1
SHA-256:	3FD27D562E32F1A052E924B6C468486ACF0B2AF42DD1AD2270E83D115D4B3F65
SHA-512:	9470EA433A7C08331FF26DF00170C81309E72145E6F32C16E7C2C1E53C54B3974B991EA128E636138F8212E276A2FDF94C344D9AB7FCEE35EC231543E08196B0
Malicious:	false
Preview:	.....3.h.b...i.j...j.v...k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....!....&.....6.....>.....E.....L.....S.....T.....U.....Z.....0.....`.....l.....v..... .....;.....w.....:.....R.....|.....B.....].....0....._.....e.....s....._.....#.....5.....=.....D.....N. .....t.....c.....~.....4.....'.....*.....^.....Q.....X.....[.....\.....p.....N.....h.....t.....?.....d..... .....*.....>.....R.....\.....].....9.....e.....w..... .....".D...%.{...(.....*.....+.....,.....F.../.t...0.}...1.....3.....4.?...5.t..6.....7.....8.B...9.f...;.....<.....=.....>.....?. ....@.....A.j...C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\bn.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	933489
Entropy (8bit):	4.282415724780387
Encrypted:	false
SSDEEP:	3072:MtVVy6YHuQ4qxkVxCp2tUkbBb5OMDK5f0Xl+IP:GVVMH5ECAt5Bb5i5lIR
MD5:	BEA57AB3921250FF4DADC9F42F8202D9
SHA1:	ACE7FC0579A946D32419E8C5FF9BC64D40E53364
SHA-256:	2BB70DC94361267E755169DDE430EA31AA21B4DAF31B5EED78901B27BC596A2E
SHA-512:	164F5C081BF23DEF7378450DFAF4DB1CEB49595351DE5D933375D9B1B409F7BC2DC96C4F228A7F024B7AC891A27603EC174EE8B3A7937BF678D61FDCD3E4C7 A8
Malicious:	false
Preview:	.....9.h.V...i.g...j.s...k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....$.....,.....4.....9.....A.....H.....O.....V.....W.....X.....].....<.....g.....y..... ..C.....".....T.....E.....s.....6.....L.....[.....}.....K.....'.....*.....6.....c..... .....`.....#. ...../.....[.....w.....C.....;.....).....B.....n.....4.....c.....&.....9.....d.....{.....3....._.....w.....J..... .....-.....?.....n.....!.....;.....i..... ....."....%.3...(.o...*.....,...../.!...0.(...1.....3.....4.....5.}...6.....7.9...8.....9.....;.....<.....=.9...>.q...?.....@. ....A.#...C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ca.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	440995
Entropy (8bit):	5.425459727706433
Encrypted:	false
SSDEEP:	12288:q86RFXgkI0h7nyRhIs3cSlFEYLCJBqB3nbhjJOtJuwIwSGMwFdLbpuQ16BtryBtE:r6wkj0RpTHpEMNJ82kLl25exte
MD5:	2CDDD012546CAF0AED6775CDF5CFDEE9
SHA1:	CACCE951770FEEFD1BCF89DE5BE97BB39606E7EE
SHA-256:	02D60B97F70C31F5C5003108321FC3AC3C79BF39A36392C3ADAF7735B9CC1C1D
SHA-512:	B75D9B2946B11B9FC7430C5773835422AAE6E716504D7841C1B08413EC18D454D9D6FAA5ED63E19C59AB2E1EE919822283FD7E21A97F54482685D541E4DD251
Malicious:	false

Preview:	.....8.h.X...i.`...j.l...k.{...l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....$.....,.....4.....;.....B.....I.....J.....K.....M.....v.....@... ..^.....`.....d.....%.....?.....O.....m.....,.....?.....O.....R.....U.....^.....r.....)......6.....=.....O.....^. ....o.....A.....b.....k.....|.....C.....J.....M.....N.....W.....`.....h.....n.....F.....N.....4..... >.....I.....N.....d.....?.....X.....].....g.....x..... ....."....%.....(.....*.....+."...,@.....j.../.....0.....1.....3.....4.....5.....6.K...7.\...8.p...9.....;.....<.....=.....>.....?... ..@.....A.....C.7...D.@...E.t.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\cs.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	452001
Entropy (8bit):	5.861977668406352
Encrypted:	false
SSDEEP:	6144:Ym4rbeY08bI70wXaNA2MXQC5t8VNDKNDZs1X8Qb:AraWbE0wqUXQC5t8VNGNDab
MD5:	6D43974C98037EECEE8691520DE4D63E
SHA1:	E15672B3AB22A059B976D245EA3F59D35C3387D1
SHA-256:	C1020222B90558A6A8A07F24756B183594641EF77562D35E7899E1489D0EBD8E
SHA-512:	64E76499D56C3E32CC013BD05E2D3EAF5618527B8035BD5A37F5018A1E6072CDE4A06F7C66921B9B087E60FF686ED63B7321F0295A34451443797FFA8E5CEA35
Malicious:	false
Preview:	.....G.h.:...i.B...j.N...k.]...l.h...n.p...o.u...p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....$.....+.....,.....-...../.....i.....y.....B... ..W.....Y.....].....*.....F.....V.....o.....~.....=.....C.....M.....T.....n.....$.....*. ....:.....S.....i.....t.....;.....`.....f.....r.....~.....!.....".....\/.....<.....C.....N.....Z.....).....\/.....)... ..6.....?.....I....._.....N.....j.....q.....{..... .....".....%.....(.....*.(...+.+...,.I.....f.../.}...0.....1.....3.....4.....5.....6.J...7.^...8.t...9.....<.....=.....>.....?.....@.....A..... C.>...D.P.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\da.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	410088
Entropy (8bit):	5.4699188226784
Encrypted:	false
SSDEEP:	6144:+/1dB4b3HibjZWsnZwlFkuJwZjUEbUSovDHv50Sr+zOUPOd40TWwd:IBa3HibtW23UtR5DrJT1
MD5:	BA54E3345D61D5CF431DB6A0D649F792
SHA1:	32B2EDC19DF7E14E6567E0FAF671C038F78A65DA
SHA-256:	DAB543BCC1A8ABF057F720F9F448E45CA5CFD1C424826BCE8933174BB2ECCAD7
SHA-512:	5F858C4C876E1D15D4929464B7D9BC2CC497EEA93D887C3CF0CC1C651A0F5A81D75F04F7A0B4277DC43BD9DEB148D147D35FA1AA2DD218D404FA2C8C389E(B5D
Malicious:	false
Preview:	.....!.(.h.x...i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z. ...|.&...}.8.....@.....E.....M.....U.....].....d.....k.....r.....s.....t.....v.....8... ..Q.....S.....W.....,.....C.....S.....Y.....a.....q.....!.....;.....R.....i..... ....."....5.....e.....n.....).....,.....9.....F.....Q.....e.....w.....:.....y.....}.....#..... (.....2.....4.....:.....H.....e.....|.....,.....0.....9.....H.....[.....e... .i..".q...%.....(.....*.....+.....,.....\/.'...0.1...1._...3.k...4.....5.....6.....7.....8.....9.....;.....<.....=.#...>.7. ..?.@...@.N...A.....C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\de.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	438111
Entropy (8bit):	5.526975973295078
Encrypted:	false
SSDEEP:	6144:uozFfPighra5V8U/x6P3T7H2mAyRc5rRRNnOIyCLM:umagpaov7H295d9yCLM
MD5:	46A45FB8E7880802E1624DF86D254973
SHA1:	13778B3BF0101C3894FCB228080C25EBD47DC046
SHA-256:	6283EC48CDDD08C387A36EC71FFF87C2AB0EF27449E8971EBA2D76A6136B1708
SHA-512:	FFA8EBAEBB3F057440176F123442B13B6F96842B9688EFE6633C0014F0DCDE982E667B0F2DC84A1F6450E310A8E05A13E35DDC24B1DE8D25BA5A711D8B07D3 7
Malicious:	false
Preview:	.....h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.'...v.<...w.l...y.O...z.^...|.d...}.v.....~.....#.....+.....4.....M.....U.....^..... .....$.....7.....C.....k.....V.....j.....q.....|.....+.....T.....}..... .....U.....f.....&.....=.....@.....S.....i.....}.....].....+.....A.....k..... .....F.....d..... ....".'...%.O...(.I..*.....+.....,.....\/.....0.....1.....3.....4.9...5.U...6.....7.....8.....9.....;.....<.....=.....>.....?.....@.3...A.\...C. {...D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\el.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	793613
Entropy (8bit):	4.758129188588161
Encrypted:	false
SSDEEP:	24576:rolquNwPB02/grQWjs6dJoaEA3HsiEcBCJ7391Qf26tKMaBlSEf5xXbW1rk2Pcjb:rMquNgB02/grQWjs6dJoaEA3HsiEcBCF
MD5:	7F92F844B9D8BEF68DADBDB85A084BD6
SHA1:	96C508FC2B624FE9C2945E2D673A645FE39AD3F2
SHA-256:	87F0A26D73FEA2EBB5017A95E937E08D7C347BAECBE93514C1B866C1E28DEA32
SHA-512:	D47EB475F9CA60BC1E7EC33FE2E2A395BB8EF3F109BC4B769FC2E03E2DDC04BB3391B10F1B382B7497555E36EF02FCA31CD47F67C03DE43D275BBDDC3BD8E7AC
Malicious:	false
Preview:	.....1.h.f...i.n...j.x...k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....#.....(.....0.....8.....@.....G.....N.....U.....V.....W.....Y.....@.....T.....}..... .....9.....;.....?.....g.....J....._.....v.....D.....j.....]....%.....Y.....L.....!.....)... ..0.....]....h.....l.....M.....P.....s.....J.....Q.....T.....U.....q.....b.....8.....l..... ....2.....e.....~.....6.....].....@.....#.....J..... .....".....%.....(.\...*.....+.....,...../.:....0.a...1.....3.....4.O...5.....6.....7.....8.k...9.....;.....<.....=... ..>.:....?.K...@.I...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\en-GB.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	356704
Entropy (8bit):	5.538284738283312
Encrypted:	false
SSDEEP:	6144:ZYAo1l9QMP9eKZwdfaY0tQWj5izSiBHXV:i5QMTZwctV5USsV
MD5:	A32F3F357725FF256BE9026398A1CD06
SHA1:	CF492E3E5C18E9E8C8CDD6B964E987541CC46505
SHA-256:	914B7BEC10C1E8C2A9E461EDAA498B2B344AADC130A30321D4116CE0C4C99AD3
SHA-512:	A96B2B00AD6883C205224770BC2CFCC93A5CF29B41BC8169117771F36264A8A89AD4E5BDDC0C50F85C0979F3355188BA86C915F0B3B1013B3ECAC9383FA8B192
Malicious:	false
Preview:	.....|...h.....i.<...j.H...k.W...l.b...n.j...o.o...p.|...r.....s.....t.....v.....w.....y.....z.....|.....}.....%.....&.....'.....,.....T.....a.....p..... .....).....@.....D.....O....._.....f.....r.....<.....O.....S.....[.....g.....t.....x.....{.....$.....). ....2.....=.....Z.....a.....p.....+.....4.....=.....G.....U.....h.....k.....|.....8.....e..... .....!....%.....5.....P.....i.....%... .)...".2...%.R...(.i...*.....+.....,...../.....0.....1.....3.....4.!...5.8...6.j...7.z...8.....9.....;.....<.....=.....>. ....?.....@.....A...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\en-US.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	359427
Entropy (8bit):	5.527720379525449
Encrypted:	false
SSDEEP:	6144:hVewV1XEsUrS0MP9eurM9faYkuiEB53bS3nwgfwi:BQo0MPrMsuD5LSjfwi
MD5:	06D28839EA0B3AAB4597BA8646A53A96
SHA1:	9C6A74AAE8C783546D613C6F38CBFC8F5E3736F1
SHA-256:	69C1A2E1B30D83612DECF1A8DD7B124A04F58E9F2465876726F02F7F7D5EB54A
SHA-512:	A432542DC98795CE0EA6FA4A6BBCBAE8BA126F1FDA025A9AD6FF3FA67EEE85DCF7AFC6678F5100BB1543C4D00AC75043EA92E64B65C9EF6BD946CE3DC4D5AE71
Malicious:	false
Preview:	.....h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y. ...z./...|.5...}.G.....O.....T.....\.....d.....l.....s.....z.....3.....D.....F. ....J.....r.....!.....4.....8.....>.....N....._.....h..... .....5.....H.....].....i.....n.....v.....}..... .....&.....6.....d..... .....4.....;.....>.....?.....F.....N.....V.....].....b.....m.....+.....6.....Q.....W.....i... ..m.....w.....|.....;.....P.....T.....[.....f.....x..... .....".....%.....(.....*.....+.....,...../.....0.&...1.Y...3.g...4.{...5.....6.....7.....8.....9.....;.....<.....=.....>./...?.7... @.F...A.s.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\es-419.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe

File Type:	data
Category:	dropped
Size (bytes):	435501
Entropy (8bit):	5.403603956967449
Encrypted:	false
SSDEEP:	3072:gZ/k72wvCDFb9D8jzsHYrtdy58d8pdxkoHQ7o0wryQ1KOP/5+lBFy0GLFL5RRIHm:gZ/k7dCRb9DVYzkpx/rT5aqLFL512Rdq
MD5:	C753CB5296CC411AE72964735CE0DE78
SHA1:	4151545BC2CB9FE4330F3B238AEB28E9FF0DBD6C
SHA-256:	5FCF21564CEEC93EB64D2002DE165A55C1875859975E0BF9035CBE96F258B50D
SHA-512:	5688E1F406125F939840E8308D950A741A02EF24A006FD3619F3E943595630CE32010B51BB7A37768F1C595F4C77B104BB7483CA24FF599EB04434974D894C1D
Malicious:	false
Preview:	........-...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.!...z.0...|.6...}.H.....P.....U.....].....e.....m.....t.....{.....#.....+.....O... ..f.....h.....l...../.....?.....P.....p.....8.....>.....K.....a.....v.....|.....C.....h.....x.....~..... .....%.....2.....N.....Z.....A.....Y.....q.....X.....*.....[.....j..... .....0.....R.....q..... .....",...%.P...(.i...*.....+.....,...../.....0.....1.)...3.=...4.[...5.~...6.....7.....8.....9.....;.....<.....=.-...>.I...?.S...@.h...A..... C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\es.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	435652
Entropy (8bit):	5.372028150641041
Encrypted:	false
SSDEEP:	6144:XJi0HwWCjWU7xXF6++uTtgcRzpJ2xP3n/j35f6UrC7JKoWeM66PZqC:X0qwWCjWAQMn9pcxP3/j35HrfoW5GC
MD5:	C9E0B58F2D9E087B2E8E92D31BE2A3E6
SHA1:	59A43B7021860DB2D2A7FE8CED8FD1A4B0C8322C
SHA-256:	468E0143C978A948C62D4A3DC743099A4147D39773A6112B303692D0E335810E
SHA-512:	16160E6375FDDE1EC2E17BA8622C9C953A46372143D0B09A33EE55852B2B9F037C1C16DD5BB6BD1F2454559DCB172C8317AA8B6C6B26D44E8DA706EB16EC5F 07
Malicious:	false
Preview:	.....%.$.h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.%...}.7.....?.....D.....L.....T.....\.....c.....j.....q.....r.....s.....u..... .....(.....L... ..d.....f.....j.....>.....N.....I.....#.....)....6.....C.....X.....^.....a.....g.....~.....R.....b.....h.....p.....w..... .....5.....H.....x.....0.....H.....`.....t.....{.....~.....P.....'.....[.....j..... .....H.....d..... .....".....%.6...(.S...*.r...+.u...,...../.....0.....1.....3.....4.5...5.T...6.....7.....8.....9.....;.....<.....=.....>."...?.,...@.A...A.t... C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\et.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	393348
Entropy (8bit):	5.481895721213982
Encrypted:	false
SSDEEP:	6144:5zlBfny9yawR8+qH2LxVu03ybwXfNYJYT/RyTKiYGT5Yjz43BvLCsPQ5bm:plBly2HQlIT5YjtC
MD5:	CCD361017778964DE23BF1D741CB888A
SHA1:	5B0305538762987901B7A8332635F3D7996C09DD
SHA-256:	41883AF1E49CC180FB48E02659E75B0169D974D77373CF7BB2A4EA02DD654E26
SHA-512:	A9D7C99C07229D382E8BA7CC3199BC66FC39DF5FD9B58E6A76E423B865F8C05F53398125A17A20C27462B2DB595F3D778B4D94B1853121D8447B771F9284E5C
Malicious:	false
Preview:	.....h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.%...y.+...z.:...|.@...}.R.....Z....._.....g.....o.....w.....~.....+.....5.....K..... .....$...../.....S.....c.....u.....,.....<.....@.....C.....J.....^.....q..... .....2.....H.....S.....\_.....$.....0.....>.....Q.....T.....d.....t.....3.....s.....!.....U.....a.....l..... p.....z.....*.....S.....m.....r.....z..... ....."....%.....(.....*.;...+.>...,.\.....v.../.....0.....1.....3.....4.....5.....6.>...7.U...8.n...9.....;.....<.....=.....>... ..?.....@.....A.....C.6...D.E.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\fa.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	644205
Entropy (8bit):	5.0379329694685175
Encrypted:	false

SSDEEP:	12288:YbNHatX0nuyabufwH0wNUWGOufStQ4vy1BeFtDmxJVlwjwMTAKzIxRAQiHedNu3v:YJbuyabufwUwNUWGOufStQ4vy1BeFtD6
MD5:	87A2305436BAD7556FE7ABB68767802A
SHA1:	0EDAD3677B0872321A1F8F3D391C17AB373ABA17
SHA-256:	9068DC6C71FD8BBC1A4F3B2009689472D1FD2C096B7E8AFB3E089A46B98D8B38
SHA-512:	6C32B1C83E03B553843FAABB5A9C1B63C769B13DE60841D2BC81F2C9514B30EBF16551ACF33262EF8ABAA4A5AA3955600A35A045B0FD446964109C58A2734969
Malicious:	false
Preview:	.....p.h.....i.....j.....k.....l.....n.!...o.&...p.3...r.9...s.J...t.S...v.h...w.u...y.{...z.....|.....}.....+.....E.....a.....2.....Y... ..\.....d.....*.....W.....2.....I.....b..... .....<.....B.....Q.....W.....f..... ..../.....;.....Q.....R.....E.....b.....^.....q.....h..... .....:.....[.....<.....a.....k.....q..... ....."....%.-...(.W...*.....+.....,...../.....0.....1.]...3.I...4.....5.....6./...7.g...8.....9.....;.....<.....=.....>.....?.....@.8...A. ....C.....D.....E...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\fi.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	401959
Entropy (8bit):	5.449269956526462
Encrypted:	false
SSDEEP:	6144:MYecIeTKohFeI4OsOSFOEi3paUXJLY5gYuyHsEl18OWUcl0wwPKNbX1wAEb:1eT0Z15av5gY1HsEl18OWUkzEb
MD5:	F87A1CCBCF3DB6988E95E94333BC5A4F
SHA1:	E85F8446EB74D8BD4318354EC98135C17AFE3248
SHA-256:	052A72C9D6F2BB55F02FB1C5C4C68525A32B8CC9120C270D07D7B813D604F7DC
SHA-512:	C4A7EE0552B343010FCE8CEEEF70620ACF672C9AB56FC24CCFB88ABDBAD23AAC4CEE65C8B241C594B7EC92D0841087485AEDA583D2E887CF4C823A10B2E7CD3C
Malicious:	false
Preview:	.....r.h.....i.....j.....k.....l.....n.#...o.(...p.5...r.;...s.L...t.U...v.j...w.w...y.}...z.....|.....}.....!.....2.....E.....K.....T.....q.....x..... .....!.....>.....C.....Q.....[.....j.....v.....<.....I.....Q.....X.....j.....7.....S.....].....b.....j.....q.....}..... .....K.....m.....u..... .....#.....$.....-.....5.....<.....C.....R...../.....7.....~..... .....(.....D.....`.....(.....0... .;...".N...%.z...(.....*.....+.....,...../.....0.....1.V...3.d...4.....5.....6.....7.....8.....9.&...;.L...<.\...=.h...>.~...?... ..@.....A.....C.....D.....E.4.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\fil.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	453534
Entropy (8bit):	5.215241054251821
Encrypted:	false
SSDEEP:	6144:lHFro0m4qhQiy6DQejOQ5V/xe8zGUZ3Lms5lXmJlLATyiH:lHhrm4q5/5T8s5lmq
MD5:	2E6A6728BD5A09339AC01A38BF686310
SHA1:	619E27F30C99EFF8F2DF3BA2287C6F7FE0B5B063
SHA-256:	E8F03C2E9C88ADB04648EF93F9EA3CFF87641638AC97C9A6752B751E7F7A8A20
SHA-512:	0452AC74EAFCF971265DE92041659C006B5E559919B895B41795BB1307EE7C302E873440B006485B7CFFCDAB0F6B908A119683FAB40A664D5BF3591239427C00
Malicious:	false
Preview:	.....h.H...i.^...j.j...k.y...l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}....."....*.....2.....9.....@.....G.....H.....I.....N.....u..... ..1.....3.....7.....`.....s.....'.....J.....]....e.....o.....4.....G.....O.....R.....X.....p.....!.....&.....5.....<. ....M.....[.....x.....$.....W.....E.....^.....y.....Z.....$.....N..... V.....j.....n.....{.....5.....U..... ....".....%.J...(.c...*.....+.....,...../.....0.....1.....3.....4.;...5.\...6.....7.....8.....9.....;.....<.....=.....>. &...?.....@.A...A.v.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\fr.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	470901
Entropy (8bit):	5.402862426852591
Encrypted:	false
SSDEEP:	12288:DVJxu/lk6QuamV1ilzaWO8ZQMYnYMFQaBIWKe5Xxkq20wCszvZL2vULN1oThXn5r:rxUjVrszc5jn
MD5:	8E21CEC6CB5732FD2BAA28F3E572EF7D
SHA1:	778228DEE97F5475B9982375740D6F90E8E5FE0C
SHA-256:	CD21CAE54EB6CB115771D1AFE14D17822E13332759F8710D6386A6E4277C11C8

SHA-512:	07726AFA312F6104E3D92C6BE13FC4B0E728A4A21F643C9552A961784063D3C8A9C52E5649FFAA9FD6A083DC5DE37316E0D2CC10CD1A6FBEB83789C385AE99B
Malicious:	false
Preview:	.....C.h.B...i.S...j._...k.n...l.y...n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....'.....5.....<.....=.....>.....@.....e.....u..... .....l.....l.....\.....z.....A.....]....._.....r.....".....%.....(.....1.....l.....[.....l.....%.....3.....F.....e.....m.....}.....=.....f.....x.....?.....F.....I.....J.....R.....Z.....c.....j.....}.....A.....H..... ..#.....'.....A.....f.....P.....g.....n.....w..... .....".....%.....(.....*.*...+.-...,K.....b../.....0.....1.....3.....4.....5.#...6.o...7.....8.....9.....;.....<.....=.....>.....?.....@. &...A.e...C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\gu.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	907786
Entropy (8bit):	4.3275112767972574
Encrypted:	false
SSDEEP:	3072:+Np5emhl6KNyUrBh8PITmKMaW4eeenbssMhmksd4t+0+z20QmuOAl5dUjvawWnhG:+NpXI7gHJxt8sW5cZhcxl+
MD5:	0C33E2A35EAAED3572F31E7B24D4493B
SHA1:	278498568109EA7D6CB34C634316F95B04155B64
SHA-256:	0F0FEE8A2F22F80A0C4A758E7F4FD90D40BE4048DCAB0D824135CAA5E92EFD5D
SHA-512:	4EEBF9BE5A8C317D2D2E8E9B1E607774F5C7C35AF7D8BD6C80326FE3C6E2E05089F04485EEDDE8BE8C7B71A7B49E407289F361361D86802C0463C5B6B296F2A4
Malicious:	false
Preview:	.....4.h.`...i.z...j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.).....1.....6.....>.....F.....N.....U.....\.....c.....d.....e.....j.....+.....V.....k.....Q... .....(.....^.....,.....T.....w.....9.....b.....~.....?.....K.....d.....P.....{.....T..... .....1......./.....E.....w.....j.....K.....u.....x.....*.....Q.....X.....[.....].....v.....n.....3.....y.....(.....K..... k.....t.....<.....u.....*.....a.....P.....s..... .....".....%.?...(.....*.....+.....,...../.W...0.....1.....3.....4.+...5.a...6.....7.....8.R...9.z...;.....<.....=... ..>.....?.!...@.V...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\he.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	562875
Entropy (8bit):	4.640306106556615
Encrypted:	false
SSDEEP:	12288:NiYE4ErOOFmTj2/1cH47n60/AfOX4neQCapHT5fJmodGMlv55lmi2DnwmIQgQ:Nci5EoF
MD5:	8B3957DDA3C9FD903D2C4B8A5F686475
SHA1:	36E45B4D30FD1E59ECAFE095F405E0722A814A17
SHA-256:	AD20B3D634130C247F4FF954F1A5C56687523E5610F2EC6085E257126C4513A4
SHA-512:	1DD54CE0A1F30BA087A9D09B9AA2928DEC3070788D7DB3DC2BBD27FA6126F70FA1E05106A1503602B203FA76BE914210A38D5DC9C6BB56C56857EF08C528C4F2
Malicious:	false
Preview:	.....W.h.....i.+...j.7...k.F...l.Q...n.Y...o.^...p.k...r.q...s.....t.....v.....w.....y.....z.....|.....}.....h.....3... ..P.....R.....V.....~.....0.....r.....&.....w.....4.....Y.....u.....5.....J.....T.....\.....c.....o. .....".....5.....Q.....t.....0.....L.....g.....!.....6.....@.....K....._.....$.....=.....u..... .....$.....<.....p.....8.....B.....S.....z..... .....".....%.....(.....*.!...+.$...,.B.....S.../.s...0.....1.....3.....4.....5.%...6.i...7.....8.....9.....;.....<.....=.....>.....?. ....@.3...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\hi.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	950376
Entropy (8bit):	4.316812155330309
Encrypted:	false
SSDEEP:	3072:SIYvII2+N6GbSJWbkXSvc4QAEm5dmGhsYK/GR3J+P8N06bxdYnLsuSQdnPtg83cf:SIKII9kGmJzl5d58Jy2
MD5:	4EB5C501AECB647FA81FB4B65B0CB6D6
SHA1:	5154741CCEB272352F0814850E75B517F7F8A023
SHA-256:	71830814B8C7028A114A53A4E715FFA8DA12F01D920455242A0CBC35FEF48E6B
SHA-512:	2BF32962D4F018959281F6F09D149AADD901C21131EF25AA1199ECD73DC16E2377EEEB67352E030198AA280AC1FD5962EB226FC6481C654D8D332751A20329D
Malicious:	false

Preview:	.....f.h.....i.....j.....k.(...l.3...n.;...o.@...p.M...r.S...s.d...t.m...v.....w.....y.....z.....|.....}.....Y.....|.....&.....(.....,.....T.....;.....N.....4.....8.....c.....9.....R.....a.....#.....i.....#.....D.....d.....l.....%.....U.....~....._.....?.....`.....B.....X.....-.....j.....(.....K.....]..... .....;.....J..... .....F.....n..... ....."....%.....(.O...*.....+.....,...../.7...0.N...1.....3.....4.,...5.Y...6.....7.....8.S...9.x...;.....<.....=.....>.....?. ....@.Q...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\hr.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	438400
Entropy (8bit):	5.534888254866354
Encrypted:	false
SSDEEP:	3072:AVgFY01/7xHaZURnmgHqbKPOS+7Wr/5cIG0uPXQ1lF6Wk6DkYAiKbeM/MQbngt3a:AVYB1/7YKAOa5/58178pjcO
MD5:	23FDDE99818BA28131A6BA81DECF2C1B
SHA1:	C1A87661F80C7DDE9A08A360D2F5B72F58042076
SHA-256:	08FC2B1E6B9652D809A7550F1343B3EE54EBCBAD0FE74B009AAB6EF926C0279B
SHA-512:	0F53B131D142C7B88081AFA59F10E17BE489C342F2E328D0E7BCAA18B5DCFA599B37CA09317AA9AE564E52A3CEA06D79021EAC6AB5AB38A9C0EC99BDCE797E9E
Malicious:	false
Preview:	.....5...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.&...w.3...y.9...z.H...|.N...}.`.....h.....m.....u.....}.....#.....7.....K.....p... ....B.....T.....c.....z.....&.....:.....?.....B.....H.....\.....n.....~.....&. ....2.....H.....\.....g.....~.....@.....L.....]....h.....|.....)).....5.....:.....B.....N.....%.....q..... .....'.....-.....B.....I....."....6....>.....H.....V.....x..... ...."....%.....(....*.....+....., ...9.../.K...0.Q...1.....3.....4.....5.....6.....7.-...8.G...9.f...;.t...<.....=.....>.....?. ....@.....A.....C.&.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\hu.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	472048
Entropy (8bit):	5.652811013920142
Encrypted:	false
SSDEEP:	6144:xaFSpYjWPSoLaIAetky1+n5QgsZfGRtgY6mHHPSim7WwQGeDCd5gRRVJtGNvw2nZ:UxiPLAZn5QgZrH+7UdCd5v1Z
MD5:	2FEF83993A62F73F8E4B40A6E28A085C
SHA1:	8BAE181F3EED8D5EA8FB0F912C679E608EE7C008
SHA-256:	CA4B4C7C7BE45EA0871ABF7D5668AB948F712A02FACDC1D6BBC189B1B3522446
SHA-512:	6EED29ACD38B662F62381A5C00EBFB254915A57DE6FDE8E6DA77F60DFFD13D4846B26B1897D710EF852BCEC5728A4460BECAED2367F1A06A066DA77521701324
Malicious:	false
Preview:	.....K.h.2...i.C...j.M...k.\...l.g...n.o...o.t...p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....#.....*.....+.....,.....1.....p.....<... ..P.....R.....V.....~.....0.....@.....Q.....|.....5.....;.....E.....]....|.....<.....d..... .....[.....f.....~.....5.....8.....P.....e.....,.....Y...._.....!.....G..... O.....].....e.....k.....*.....b..... .....".0...%.Y...(.v...*.....+.....,...../.....0.....1.1...3.=...4.Z...5.|...6.....7.....8.....9.....;.%...<.-...=.7...>.L. ..?.Y...@.I...A.....C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\id.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	386866
Entropy (8bit):	5.400536677864927
Encrypted:	false
SSDEEP:	6144:CuI7Z20J6S8IZMGqv00FU/XfjDVnjHFTRmPbUK1E5+shlvtmZSVsEaQm:jyI6SmMq0iXVnjHFNmDUsE5+shPm
MD5:	0DCB56F6B196199F7ED802C06B774037
SHA1:	F62EDD5E814D05CC4AEB5574FC63ACFDEFFB6010
SHA-256:	BD512E36A88F0D7E6FECC0B559ADB2761589947FEF9C253DC350CD8D6EA889F2
SHA-512:	E03474255BCE20004788475EE1F546EE7830E9B9960023B15210D88347032B5376848AEADEF3E953EC654D3905BAEE37279BFAA287AF7669CA66E382A4B1344C
Malicious:	false
Preview:	.....7.h.Z...i.k...j.w...k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....".....'...../.....7.....?.....F.....M.....T.....U.....V.....X.....{..... .....8.....H.....i.....q.....'.....5.....F.....q.....+.....H.....f.....t.....y..... .....l.....0.....K.....Z.....".....1.....H.....].....n.....u.....x.....y.....=.....A.....v..... .....6.....[.....p..... .....".l...%.F...(.a...*.z...+.}...../.....0.....1.....3.....4.#...5.5...6.k...7.~...8.....9.....;.....<.....=.....>.....?..... @.....A...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\it.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	427761
Entropy (8bit):	5.3083167597834064
Encrypted:	false
SSDEEP:	6144:7G169R9ACcto0SgqRrhsO1F+RT9TeexAGT95ELRqbKYT9fLwdQ2Yoi4Z8Hr21GWg:7A69RCi7eZh48CfilwLq58zoP
MD5:	47C89F9BA4993E7CB6640C23F444E9CD
SHA1:	0E3755D2835742B7AA4E1D5245454F7CF22A2D47
SHA-256:	95BBF94625CF0476124763CEBEDCF5EE46148BB6B5C006F86540A02E8D8C883C
SHA-512:	948E4DA235CF7D0272FD7A99E7238596E5D50913886FC73FE35F9AF17D1087F550A3CC3251EE6595F9872EF0B88E75725405382E6AEA4850088E068D5B80922D
Malicious:	false
Preview:	.....2.h.d...i.u...j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.$.....,.....1.....9.....A.....I.....P.....W.....^....._.....`.....b.....(... ..9.....;.....?.....g.....z.....8.....N.....R.....g.....}.....#.....*.....>.....T.....h.....(. ....7.....N.....V.....d.....1.....=.....D.....P.....c.....x.....{.....!.....+.....1.....A.....^.....s..... .....#.....<.....o...../.....;... .>...".H...%.I...(.....*.....+.....,...../.....0.....1.8...3.L...4.I...5.....6.....7.....8.....9.....;.(...<.5...=.D...>.o. ..?.z...@.....A.....C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ja.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	523066
Entropy (8bit):	5.701694810920732
Encrypted:	false
SSDEEP:	6144:I5Q+c9x+7+YqFkl+cDWSJ7sZDs29v3rbP5BgLTxVx:I5Q5yqCl/JsZDs29v3f5BgLN
MD5:	AFD423713E28B3980392443F31DBDA7B
SHA1:	926560B21AF422F22E1CCA1A4A2948FF988BC6D9
SHA-256:	88383DDCCACB53F3CE5918CD80B5DAFB16B3CF1FAB295E230CC15490600615E4
SHA-512:	1544F7A91B4B63BB80F651833A931204E44745BB0BCCFB5564EE9AF3149218F140B6ADFB6D4EBB5CE5E82F5C345C098CAE8A0637B274C42F6711AA53877B0BD 4
Malicious:	false
Preview:	.....d...h.....i.....j.....k.#...l.,...m.4...o.I...p.V...v.\...w.i...y.o...z.~...|.....}.....2.....K.....i.....@.....a... ..c.....g.....;.....b.....r.....w.....'.....Q.....{.....;.....K.....T.....\.....c.....l..... .....$.....Z.....{.....8.....\.....\_.....n.....!.....$.....-.....6.....<.....l.....\.....2.....&.....>.....q..... .....O.....g.....&.....;.....[.....a... .j...".|...%.....(.....*.!...+.$...,.F.....b.../.....0.....1.....3.....4.....5.-...6.....7.....8.....9.....;.....<.....=.#...>.R...?.\...@.q...A.....C.....D. ....E.....F.H...G.r.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\kn.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	1047678
Entropy (8bit):	4.233435530912806
Encrypted:	false
SSDEEP:	6144:3jIXOpf5AEb7XtwKG20PSjNlB2DPVX1EB/lthEVGkcVw27zidmaZXH0r2AxiYRpv:3cHS7XxRPaEjJ2j7q5DPUc+vB+13d
MD5:	74F0E9C7C670A981D3651E0D189DFC47
SHA1:	A2FD3037311F36AAA348805D57172F9E9B0680C6
SHA-256:	0C8E0B6A8398D7B9AB9CAC634E4A7CE4453540358E79AC6E9C5633EFB4182FE9
SHA-512:	2C555439F7DE3902B2B1A940CD43977558C4D9239C449105FC24777952AF8DE592BA86A7476567D190719C66D38F7A7982C9B94278C0594DE1B427DC546F2D89
Malicious:	false
Preview:	.....6...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.(...w.5...y.;...z.J...|.P...}.b.....j.....o.....w.....5.....l..... .....t.....j.....l. ....x.....1.....L.....<....._.....Z.....X.....-.....[.....s.....{..... 3.....H.....w.....C.....7.....8.....6.....s.....3.....Q.....d.....%.....P.....k.....V.....-... ..?.....K.....N.....%.....e.....8.....M.....k..... .....".e...%.....(.....*.f...+.i...,...../.....0.....1.....3.....4.....5.]...6.....7.....8.\...9.....;.....<.....=.....>.7...?.J...@. ....A.....C.a...D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ko.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped

Size (bytes):	439630
Entropy (8bit):	6.085011350313488
Encrypted:	false
SSDEEP:	12288:4ysgl3zGY/cUXcfyC8OhOJhmHCqq5A72eEd8MtKq7hUoXAj:l32WJ75z8AAj
MD5:	C90A42BB27BCBF1BD345DC998F9E410E
SHA1:	66F8BB72DB6B38E2D288959BCEE3C43CAEFDC59A
SHA-256:	56100D20A59FE6CB333F57FFDEF90157324AE1B90194E852478DAA8C46D29DE9
SHA-512:	B5912C895A6A3B391555EFC10B15D45FE9A84473C8687327B7D2FA033711E437E2F160345DAEFD554374357E0AFBAEDA4A25F4F69CA74E498D7081062F299B46
Malicious:	false
Preview:	........H...h.....i.....j.....k.....l.....m.....o.....p.....r.....s.#...t.,...y.A...z.P...|.V...}.h.....p.....u.....}.....$.....-.....:.....T.....a.....i.....)....5.....B.....R.....Y.....s.....Z.....p.....v.....<.....`.....V.....l.....y.....B.....O.....d.....x.....{.....n.....:.....C.....,...../.....B.....H.....Q.....h.....T.....d.....m.....s.....".....%.....(.....*.C...+.F...,w...../.....0.....1.....3.....4.+...5.S...6.....7.....8.....9.....;.....<.....=.....>.....?.%...@.9...A.g...C.....D.....E.....F.....G...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\lt.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	474696
Entropy (8bit):	5.648556930784026
Encrypted:	false
SSDEEP:	6144:mGUgXQKlF4q4RmoBkzMbI0COOeQ0AI7U5FJzvnhJaIV9Jx62cJ2I96Sut:maQK4NnbhCOOe495PzvnUJx6nP6Sut
MD5:	06D8DB8AAB68C565AF14BFE408AE4DAF
SHA1:	0898FD0EE4D7380B93B8FB3D4A1816EB810EA9A7
SHA-256:	ECB4ECBD96575F6F984F60E85AB1EBB0067E73174FF9912941EE1AAA28516D93
SHA-512:	1EBC04CCA7E3BF005F9BEFAD5A81736FC572383A636C7237E4206E75B05BEFE49F967427F912C97758AA392F9CC2DCBDF07C471562CB4CCC90F7D8E951C3AE9F
Malicious:	false
Preview:	........".'.h.z...i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z."...|.(...}.:.....B.....G.....O.....W....._.....f.....m.....t.....u.....v.....x.....$.....0.....E.....d...u.....w.....{.....$.....T.....f.....u.....*...../.....9.....V.....t.....8.....^.....+.....T.....g.....r...../.....2.....H.....[.....m.....A.....@.....^...../.....h.....|.....,.....C.....J.....R.....l.....".....%.....(.....*.'...+.*...,H.....t.../.....0.....1.....3.....4.....5.....6.k...7.....8.....9.....;.....<.....=.....>.....?.....@.#...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\lv.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	472357
Entropy (8bit):	5.648594391725834
Encrypted:	false
SSDEEP:	6144:k6nCZt8n4UUaNHkt9NLtVFHrP47H4zRa9Y2b3L5fRZanVhE19AYFs4FjEA5FGlsW:FQMlVEzM74zWYOL5CE9DjYs18
MD5:	F8A5403BD91F231DB58E77C9D4514E2F
SHA1:	7D29E2D8459AF6FC3082CEC0D9638DAF5275BF3D
SHA-256:	DFB9B5EE446977DC0435CFF4D66402D3A9426EDB106EFFDBB7D86379527C5956
SHA-512:	F491CFFDC5CC588F7EC70F87BE84615AAF5B39E9C990CD9C835E65BEB27F26334517ABAC1AF7419F2B7B18F94C369037C8DF4C1C8E26A5FED4288D477DC0874E
Malicious:	false
Preview:	........:...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.0...w.=...y.C...z.R...|.X...}.j.....r.....w.....G.....Q.....Y.....2.....Z.....m.....0.....B.....J.....S.....d.....z.....'.....@.....H.....P.....W.....i.....u.....&.....@.....J.....).....<.....N.....g.....i.....-.....M.....M.....I.....(.....5... .>...".O...%.u...(.....*.....+.....,.....)...../.....0.....1.S...3.d...4.z...5.....6.....7.....8.....9. ...<.+...=.5...>.S...?.[...@.k...A.....C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ml.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	1091460
Entropy (8bit):	4.270211892148615
Encrypted:	false
SSDEEP:	12288:CnO59wW3g+Z/47/ZmQkg3sKMmWDcZubSAI51jy03eGhd5R/7d9gf3co:COXZdKg03eI5R/7Mf31

MD5:	FB1A6E31DFB4F4C78A50B4DBECE0E1C1
SHA1:	367C506478380F8BAB411747A906F8F8C60DF30A
SHA-256:	A7AFB3EBFA8F4D2E35DFDD5554FF2702182E73DAD0FD82F8B4207A61563ED134
SHA-512:	18AFB816E974C9F0D669AF7CB6A5D8761E1C5AF69317E6EA293559876549692BAF1567657B356BA9D52ECDF4D117B7EE7FE003D1820286470D43AF89321E3F6D
Malicious:	false
Preview:	.....9...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.;...y.A...z.P...|.V...}.h.....p.....u.....}.....N.....k.....Y..... .....X.....I.....+.....B.....e.....).....p.....<.....H.....K.....o.....>.....f.....2.....].... .....S.....B.....t.....f.....*.....Y.....\.....#.....V.....L.....h.....P.....V..... ..6.....E.....T.....).....`.....K..... .....".8...%.....(.....*.....+.....,...../.@...0.P...1.....3.....4.J...5.....6.D...7.....8.....9.J...;....<.....=.....>.....?. ....@.G...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\mr.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	891781
Entropy (8bit):	4.3007658045691715
Encrypted:	false
SSDEEP:	3072:ryyL/Ti/fQDFJEm1VhkrXspg2GLXFEMUAG3GRa3RQR3Kz/YYxi4noc4AmHwpVuQ4:pTi/fSLIje5DDcJ01V55ipWLYb
MD5:	1675668911FD3063E092FE34579C210C
SHA1:	D1D09041778599002D07A89848DDD79CF5F4F4DB
SHA-256:	436EFBDBCE605C23F855644A9FF1B04D9A3ECA37DE3B18DE8C3E589930D54096
SHA-512:	61C7AABB00700773BB55522E7AE9482D1D97ACE936C9BBFEAEF3215A976C411A51F41A2D5AA05F2B286B0D112B5616215B9FA3632EAEE38B1EC090DFB29391B1
Malicious:	false
Preview:	.....T.h. ...i.:...j.F...k.U...l.`...n.h...o.m...p.z...r.....s.....t.....v.....w.....y.....z.....|.....}.....#.....$.....%.....*.....;.....k.....}..... ..D.....F.....J.....r.....0.....b.....x.....=.....$.....C.....#.....E.....z.....).....w.....O.....r..... .....+.....:.....h.....R.....>.....T.....(.....D.....c.....4.....K.....h.....:.....I.....+.....G..... .....6.....M.....|.....\.....k..... .!...".F...%.....(.....*.....+.....,.1.....q.../.....0.....1.0...3.G...4.{...5.....6. ...7.N...8.....9.....;.....<.#...=.@. ..>.I...?.....@.....A.....C.I.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ms.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	404856
Entropy (8bit):	5.277592243066906
Encrypted:	false
SSDEEP:	6144:D0DH30N8CXsxdu2kulaBGY/H3IUv5sf3UwMM3KbI:DGjfxdflasKHL5UUDML
MD5:	2C4056D84B980267FAADD69D52C17086
SHA1:	3B3C5FCF182D86A170C8F35C041BF3869A82B362
SHA-256:	163EB7BA5F0C61ACB6443709C24E38CA6370A33F89A12E13D0A57C258A87CA16
SHA-512:	47285AB42B46CF7D6556EAC2A8F7AFB9A9C9ABE8CB026FE847B2504E4DBDDD481A98C1EA959C74E31F195ECDBB618A3D93DF8F20B797411A8BF2B3856FC9B963
Malicious:	false
Preview:	.....;...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.)...w.6...y.<...z.K...|.Q...}.c.....k.....p.....x.....>.....J.....X.....{... .....(.....=.....Y.....e.....s.....".....4.....A.....E.....H.....S.....d.....s.....". .....<.....W.....^.....p.....+.....9.....B.....M.....c.....w.....z.....!.....)...../.....;.....h.....+.....<.....^..... i.....{.....%.....=.....k..... .....".....%.....(.....*.....+./.....M.....^.../.t...0.~...1.....3.....4.....5.....6.-...7.D...8.`...9.s...;.....<.....=.....>. ....?.....@.....A...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\nb.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	396020
Entropy (8bit):	5.443726777531974
Encrypted:	false
SSDEEP:	6144:0t4+Y0qilKh+7Op7fCFegnmKQ7PpWS6j25OB4Y6GOQzMh:u4+Y0FKh+7Op7fCFkP8Vi5OB4NQzMh
MD5:	23ECCE10DB7753622FD7CD956AA55212
SHA1:	52AFFC68E91448D8AECF2396F02EDE77D4EA664F
SHA-256:	29F38D3720C948FD261A2AEA7D195E861A73A1313071BD2CBF1EBCBBA77C63E6
SHA-512:	553543BEF496052995E33E2F3E8BD66AC845351CD292623479A303261900C393CEC35AF3E0ECD57DB84197E6F7653FFA4EEAF4950647AE2D5304F961890DEBA1

Malicious:	false
Preview:	.....&.#.h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.!..z.0...|.6...}.H.....P.....U.....]....e.....m.....t....{......"....E... ..\.....^.....b.....+.....<.....Z.....i.....o.....u.....!....&.....E.....X.....m..... .....&.....;.....k.....v.....)....,....;.....H.....S.....e.....u.....9.....j.....n.....&..... 6.....H.....R.....V.....[.....l....."....5.....9.....B.....O.....g.....r... .w..."....%.....(....*.....+.....,...../. ...0.%...1.T...3.`...4.z...5.....6.....7.....8.....9....;....<.$...=./. ..>.C...?.H...@.T...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\nl.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	408303
Entropy (8bit):	5.386796049452319
Encrypted:	false
SSDEEP:	6144:lZobt+gAv/5SfHepaMs3B+qnCv+659tuxMGpe/hWUP6C:QLgAv/5SJTb659tuxMGpe/hbP6C
MD5:	54817BE286DBFD9DE461F42304EB72CC
SHA1:	79386881A11E6C7D49F2D117822C29D7631F3830
SHA-256:	3C682E37DF71CC036C2B5E91064407FED8091C0306A856121E28C19E7110E1E4
SHA-512:	D8F922B028B03C6379911308CF240D104B40A9C46F67A6DDBBFCD20110C287E8106376CD6E8295915D054E05B2A8A045B3AB8D98932C1BE97B1F258525DB1A6
Malicious:	false
Preview:	.....<.h.P...i.a...j.m...k.|...l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....%.....-.....5.....<.....C.....J.....K.....L.....N.....|..... .....!.....I.....a.....}...../.....I.....N.....W.....f.....v.....'.....>.....S.....k.....".... 2.....I.....P.....e.....$.....7.....G.....Q.....\_.....~.....$.....8.....I.....K.....`.....x..... .....0.....S.....h..... .....".....%.0...(.K...*.d...+.g...,...../.....0.....1.....3.....4.....5.0...6.j...7.....8.....9....;....<.....=.....>.....?.....@.....A.?... C.X...D.b.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\pl.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	455672
Entropy (8bit):	5.786204955993163
Encrypted:	false
SSDEEP:	12288:XEmjSoGU/h+XgvqiWHbdvP/CUd9e3maUXI0hmhF1Qhwkd54Mz4c6W/:0Zl+I1QhX5qa
MD5:	41CB68DE75D011281C7936194EF8457F
SHA1:	6BD3EFBF5142769C6FBE8478185EDF89F471716A
SHA-256:	D52358B8FD70F1F18B3F8ECC4AA9C791591DBB698EF8D8670312E50F024DB451
SHA-512:	CEB90FA9F723C3D8D522A401CB46545C72A2DDD1D04F091E9D7CA5212CEDCC641C54CB8FE19595E9C823B2ED374757E5BA7D1813CD763BBD8D726B1E2EBE 407
Malicious:	false
Preview:	.....$.%.h.~...i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.$...|.*...}.<.....D.....I.....Q.....Y.....a.....h.....o.....v.....w.....x.....z.....$.....L... ..a.....c.....g.....&.....1.....@.....Y.....j.....p.....v.....!.....*...../.....D.....Y.....n..... .....%.....7.....B.....R.....(.....2.....C.....L.....\.....|.....".....3.....y.....h..... .....$.....).....>.....c.....}..... .....7.....>.....H....._.....y..... ....."....%.....(....*.....+.....,.....A.../.V...0.b...1.....3.....4.....5.....6.....7.-...8.F...9.W...;.f...<.q...=.{. ..>.....?.....@.....A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\pt-BR.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	429297
Entropy (8bit):	5.444204703419543
Encrypted:	false
SSDEEP:	6144:Zj1SlkigJpsehea53NBXBLm+9nnI1iys55nfJkW++sRgltp:Zjj9pseAaLnN5fJLnsRcD
MD5:	4F3F65F6639AE1905FA37B9B6EE2E4D4
SHA1:	07553F41C4F8F3D105EB92B65497C4976449A6B4
SHA-256:	B4E0A6064DCFE876C819EC4B00F9857B84FF52CD3E845BD0C48E31AD43A23DB9
SHA-512:	85CFCAED8FA2026C13735E7D4B6852BF794DD4A8AC078889D5EF46EC2FF7173AE443ADDCB0B0C711F6A31F80469FC1DF5AF1A78DA6397D9DF5E33CABB354F BA2
Malicious:	false

Preview:	...../...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.'...y.-...z.<...|.B...}.T.....\.....a.....i.....q.....y.....:.....B.....l..... .....:.....S.....m.....G.....M.....X.....h.....u.....y.....|.....*.....=.....C.....K.....R.....X.....c..... q.....>....`.....j.....z.....+.....2.....5.....6.....?.....H.....Q.....X.....h.....R.....g.....~..... .....)....Z.....s..... .#...".6...%.U...(.k...*.....+.....,...../.....0.....1.....3.....4.:...5.S...6.....7.....8.....9.....;.....<.....=.....>.....?.....@.%...A.\... C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\pt-PT.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	430550
Entropy (8bit):	5.422681845738878
Encrypted:	false
SSDEEP:	6144:WPh4tRdLtMRieJVJJxhzOhxcNR8f5W75BKbSR8u:ih4tRdxU/ND75BKbSRl
MD5:	7074036013BE3839E218EC7B15D49215
SHA1:	7711AE4E96EFD4F4676A3C0281A92AF56329DEEE
SHA-256:	342381F89058BEDD809991A0B416F48642DF3C71AEA10BB13E13BC15EAAF46C8
SHA-512:	8A1E9CEFB8A64B3664D9496E2D2F76E2281B3C427FE24ECB70EE74F78778D94DEF66787A7E35CCDE6037EC061E29A6AC7FD8B4010F77B13945780E1316BB16E 0
Malicious:	false
Preview:	.....?...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.%...v.:...w.G...y.M...z.\...|.b...}.t.....|.....%.....K.....W....._..... .....+.....O....._.....r.....!.....:.....B.....M.....].....j.....n.....q.....x.....5.....E.....K.....S.....Z.....`. ....k.....y.....J.....l.....w.....*.....>.....E.....H.....I.....R.....[.....d.....k.....|.....0.....8.....t..... .....&.....G.....^.....$.....0.....N.....V... .Z...".n...%.....(.....*.....+.....,...../.....0.....1.E...3.X...4.|...5.....6.....7.....8.....9. ...;.4...<.C...=.O. ..>.s...?.~...@.....A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ro.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	445082
Entropy (8bit):	5.481204880062455
Encrypted:	false
SSDEEP:	6144:wvnUEfoHLgfnNaLF33GKoZQoA02M5Hg2obs20/qulUy:wsEaLgfnoF33GKoZQod2M5HLoA/ly
MD5:	E66343D1AF0B8F483116AD7689E7FABA
SHA1:	A245B6AA9309A7C10ACA8502CBD10D9DCBD5D8DE
SHA-256:	B7B56396806412AC1721D2648FA98A89A069D1F58D359D8E90DD1C6B8473B9A2
SHA-512:	9F6517AAE57F3D8A65D4F9B354B7ED9923C1BAB8A414B78347F4DC375707907D16D458D9D458D8FBD28F065E268E092770FBC198833315CE14E6EECFC0D3F0A A
Malicious:	false
Preview:	.....0.h.h...i.y...j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.&.....3.....;.....C.....K.....R.....Y.....`.....a.....b.....d.....,... ..>.....@.....D.....l.....".....2.....E.....g.....~.....".....)....2.....L.....h.....l.....w.....'.....U.....x..... .....'.....6.....D.....e.....u.....(.....+.....<.....N.....a.....|.....?.....A.....V.....l..... .....4.....K.....y.....(.....?.....].....i... .s...".....%.....(.....*.....+.....,...../.+...0.<...1.h...3.y...4.....5.....6.....7.....8."...9.2...;.E...<.Q...=.b...>.}. ..?.....@.....A.....C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ru.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	728605
Entropy (8bit):	4.848404287210581
Encrypted:	false
SSDEEP:	12288:FKYfeXN2hnO3j/HkwzvM/sWAhwxxe8P/XvFGGJbM3cFaPuLzUFCpWNFHWajfr69R:FtVy56687
MD5:	6092FF0430736682E24595B37B3C018D
SHA1:	9D2B9822556AB1F33861C45B2F7F4236B3EA5F05
SHA-256:	C5264FA2B485326E91D4DF7A6E39122554ED632C0C17FA1F130205ED50E2D6B9
SHA-512:	FDD960F3295C280CC57915F7CABD7FFDE0C0CDF4CF6B671748A6F5B8B39376141F2A552AFCE3E2A428BA18057FB9890DA9B95FC6B8367DBDA5430E1B205A08 CF
Malicious:	false
Preview:	.....h.>...i.O...j.[...k.j...l.u...n.}...o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....#.....*.....1.....8.....9.....:.....<.....#.....J.....T.....^..... .....C.....O.....n.....3.....j.....[.....!.....:.....U.....?.....M.....U.....c..... .....`.....p.....;.....\.....o.....6.....T.....v.....1.....X.....-.....A..... V.....d.....x.....<.....m..... .....".....%.D...(.....*.....+.....,...../.R...0.c...1.....3.....4.....5.:...6.....7.....8.....9.....;/...<.I...=.]...>.....?.....@... ..A.E...C.}...D.....E.....F...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\sk.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	459341
Entropy (8bit):	5.83612791387238
Encrypted:	false
SSDEEP:	6144:WhktQ05fPaV1kP1OOygitJeKqsf2d/5hK7LtHEMEGLxGg:WGSW41+NygiqKqsf2B5hK7LtHJJL/
MD5:	B88EC1F7BBDCF1B6690F2698B3DFF738
SHA1:	C5975DE1D66827087BBF8CF0F4B3BDA816A723E1
SHA-256:	04B179B5C3A5468F495A0620A2DBC6E312EBD76BA32B98D8CC7DAAFB46EDC21E
SHA-512:	EF30AC14B17B71F5659F33778D8C4B017127C3C5BFB593DCA919A80320A66DCF5E0A3F228DCF62B05DF5D4D6929EB5401BA9C369AFFE89CF541633BB743553F 0
Malicious:	false
Preview:	........'."h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y. ...z./...|.5...}.G.....O.....T.....\.....d.....l.....s.....z.....*.....?.....n..... .....-....._.....m.....}.....:.....B.....O....._.....e.....s.....~.....)....9.....A.....l.....P.....X.....i.....x..... ....1.....Y.....~.....0.....F.....M.....P.....Q....._.....m.....u.....;..... .....a.....q..... .....;....].....&.....0... :...".N...%.r...(....*.....+.....,...../.....0.....1.8...3.F...4.f...5.....6.....7.....8.....9....;.....<.....=.(...>.=...?.G...@.Z...A. ....C.....D.....E...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\sl.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	443886
Entropy (8bit):	5.505235500325453
Encrypted:	false
SSDEEP:	6144:4O8DqTPKIM7B2zi2i+ennbANjdnPMAm4ocyxPbPDTmAu1pHHGfXjQLO25QlhDc/6:H4qy7B2kZSSl25ytc/1rg/J1i/fzUZqk
MD5:	1B02B0834B8BBD12A77F7FFF09E1D81A
SHA1:	1898CFEDDE55AAE307F7578B88CB0BCAF61E1D52
SHA-256:	B36E1FE2405CC4B9F34587E30DA2FEADAA6F03124769B02F79333ADACADDB49B
SHA-512:	B1006053ACE6F8842E9436C94934B2E7D1B502E3DF9ECD1FE59AB39AE35E69E8F0DCFF8728AEE2C35A3A1EB7A27F0146D6113B4DE0632DBAB20EB0A37942BC4C
Malicious:	false
Preview:	.....7.h.Z...i.k...j.u...k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}..... .....%.....-.....5.....=.....D.....K.....R.....S.....T.....V.....C... ..V.....X.....\.....".....\/.....E.....R.....Z.....c.....r.....H.....a.....{.....*..... N.....a.....l.....|.....9.....J.....Y.....e.....t.....$.....*.....2.....=.....d..... ....%.....8.....c.....{.....5.....<.....l.....d.....p... .z..".....%.....(.....*.....+.....,...../.../.L...0.V...1.....3.....4.....5.....6.....7.....8.4...9.T...;.a...<.m...=.w...>.....?.....@..... A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\sr.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	682487
Entropy (8bit):	4.76829773436016
Encrypted:	false
SSDEEP:	12288:EmiMMe1Knu/SyI4cH1ANLVsewp6035sp1xAx7oC+37ZJSk/k/o:EnMMeqk9k35WxAG
MD5:	4D1EE9487F4DDFDC4471366D3965293F
SHA1:	4E53084FE0D4BF4F46EA980F7423787084152FF2
SHA-256:	B75A222DB70C3F5734A75042718DA599881D5E84CC52B332E9162F78B32F4819
SHA-512:	A44A448203CC9388D8DF4C39BE9DB5436546FA17ADD0975C18CE01EA0A5CBA142692660CE6EFBF00699793CA98AF8E392E41A07DCD9C183FE03414574389609C
Malicious:	false
Preview:	.....1...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.+...y.1...z.@...|.F...}.X.....`.....e.....m.....u.....}.....2.....W.....q.....H... ..}.....".....E.....\.....v.....6.....B.....N.....v.....E.....O....._.....x.....P.....l.....(.....C. ....Z.....|.....(.....A.....S.....v.....6.....S.....c.....>.....\.....|.....i.....7.....a.....)... ..5.....P.....Z.....~.....F.....0.....<.....P.....e..... .....".....%.#...(.U...*.....+.....,...../.....0.....1.d...3.{...4.....5.....6.T...7.|...8.....9....;.....<.....=.....>.Q...?. b...@.....A.....C.#.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\sv.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe

File Type:	data
Category:	dropped
Size (bytes):	398582
Entropy (8bit):	5.563134029307162
Encrypted:	false
SSDEEP:	6144:lWebObjmSPLUfHxd8cAkxbMUK4NLXmXQMLSOzDE/xWcqpvPb5BN5Bngbd:lWebo2Aa25P5Be
MD5:	094D69544816535E4D040EF0CE923100
SHA1:	5891CDC73BC4C112855D099EE112DA0C3E9CEA81
SHA-256:	110112C2F7FF5D3C8599036669D156E96EC19E70515FBBA3BBCB2043AB994680
SHA-512:	023037077A3482A3BF2AC076B5C00922D7039BFC2098797275465138142FEA0F97C1E003F77DE71B9AB88F786B7401182618603610C51F634AD17A123FAF5BD4
Malicious:	false
Preview:	.....N.h.,...i.=...j.I...k.X...l.c...n.k...o.p...p.}...r.....s.....t.....v.....w.....y.....z.....|.....}.....&.....'.....(.....*.....T.....e.....w..... .....8.....Q.....i.....o..... .....&.....4.....C.....K.....+.....J.....k..... .....#.....X.....`.....k..... .....#.....3.....A.....N.....`.....q.....R.....)....4.....E.....N... ..V.....X.....^.....p.....C.....].....c.....m.....}..... ....."....%.....(.....*.....+.....,.#...../.../.C...0.]...1.....3.....4.....5.....6.....7.....8.)...9.8...;.I...<.Q...=._...>.v...?. ....@.....A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\sw.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	418265
Entropy (8bit):	5.358226259602233
Encrypted:	false
SSDEEP:	12288:dmnKF5TzfMUxbQufAaRO8VUZgNArc5m3HZ+bAoe4Fahk:dmsB5mw
MD5:	BC771A0E8398E14653D9A4373A73496A
SHA1:	6E844C7DAA666640AC3093D5E51276886A0F5A66
SHA-256:	7A5D056FD317B7B60A4FBF0DF39DFDD21829F2245393A21E1DDCCF1A4E3B61FE
SHA-512:	79B916C737BC44051E6B4C0A9AFDFBA26928536034C5A5149586594454855B7074F6F8FDAEB98F0B7BDE5C3DA36D66988F683DE8961E13C9C82301676F942998
Malicious:	false
Preview:	.....&.#.h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.$...\|.*...}.<.....D.....I.....Q.....Y.....a.....h.....o.....v.....w.....x.....}.....>... ..U.....W.....[..... .....2.....=.....Z.....k.....u.....{.....5.....9.....<.....A.....R.....l.....$.....+.....5. ....B.....S.....u.....|.....T.....!.....5.....K.....[.....b.....e.....f.....s.....z.....3.....l..... .....5.....S.....$.....D.....O... .W..."g...%.....(.....*.....+.....,...../.....0.....1.V...3.l...4.....5.....6.....7.....8.....9.....;.#...<.1...=.?...>. S...?.\...@.w...A...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ta.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	1078050
Entropy (8bit):	4.0511544413469025
Encrypted:	false
SSDEEP:	3072:/IFTT2M16QygBwVWhphfT5hB7zNtRaKcA2/:/cf2GDwVWhphfT5zzNtRBcA2/
MD5:	ABF95E05D798043ABF4F2F514C0517A9
SHA1:	B8C6C1CDCBFEA03FB106C7A44385A3A8E6806AA6
SHA-256:	9CD624A97493282AFED3B9B1E848B12639234FA54C04B22128169924F9C92777
SHA-512:	AACD7439DF84EC76A3D0C69C39341B51031B66B24BE53C87F3FFBCED989B38FEE416B19DB2C3B36904EAF88F98B24E1E26F070BCC8DFB4ECC99DC7BB6F6B 11F
Malicious:	false
Preview:	.....O.h.*...i.;...j.G...k.V...l.a...n.i...o.n...p.{...r.....s.....t.....v.....w.....y.....z.....|.....}.....$.....%.....&.....+.....!.....a..... .....W.....E.....d.....<.....^.....D.....m.....L.....[.....^.....p.....U.....c..... .....h.....&.....D.....w.....\.....K.....n.....&.....i.....6.....T.....i.....|.....2.....2.....B..... G.....\.....M.....0.....h.....A.....%.....I... .X..."....%.....(.a...*.....+.....,...../.>...0.W...1.....3.....4.o...5.....6.....7.....8.1...9.\...;.....<.....=... ..>.!...?.4...@.h...A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\te.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	997284
Entropy (8bit):	4.300315130198989
Encrypted:	false

SSDEEP:	12288:4hk/xBJ3p1F96/iTlw2cTgTNFOpnr/p54JqQJgwgtaJCb8+58XfX0DDq9OyJoTA1:45kz5sMBD
MD5:	51356402AF92C1912F185B6BC9AA9026
SHA1:	60CCD65D7EF35E5219F2BD1ECED66E1BA984A8CB
SHA-256:	11DF9EAA9216B091FAB01F66FD77BCB17C0BEA0DB3EA7A803BDF5DC6C6E18322
SHA-512:	8DDC7946A9445A832B4B3B254D24E12D66C42AF8CF7DC13ADD4CD3A9AE50B83E5178830300C0B08AA145D55D79B868EFA9D95A116623044D7DF8EAC1A6556 2
Malicious:	false
Preview:	.....7...h.....i.....j.....k.....l.....n.....o.....p.....r.....s.....t.....v.3...w.@...y.F...z.U...|.[...}.m.....u.....z.....e.....Q.....r..... ..f.....h.....t.....-.....d.....p.....V.....C.....\/.....V.....h.....f.....5..... ....@.....b.....w.....5.....C.....z.....:.....\.....~.....).....0.....3.....5.....Z.....a.....8.....E..... \/.....a.....m.....~.....k.....-.....m..... .....".....%.u...(.....*.....+.....,.<.....s.../.....0.....1.....3.....4.....5.;...6.....7.....8.L...9.....;.....<.....=.....>. ....?.0...@.g...A...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\th.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	836855
Entropy (8bit):	4.34610730153968
Encrypted:	false
SSDEEP:	12288:XeYsml39by4s3/5UidrLRflssB/j86qGv0loIG2EeuLADq7Kle9dAv7y3KH409X9:XJuI5j5N
MD5:	2376DC182234C3F1188DC0D6E1840453
SHA1:	2DD35D89E79512E37B721FA697CB2E9E07A1D1CF
SHA-256:	610A440605110F1AA18B1134D116C66CD2050DA53E0360924A3171D0850C27FC
SHA-512:	7C81FE0C2172FF49B6AD9236762FE81E0A786991CA6C6E3549BD66F9CBA3C14D96F8560E01BF3681355D6155A0B1B9CB5FA0177137F71BA3D8A1FB6FDED29E3 8
Malicious:	false
Preview:	.....Z...h.....i.....j.....k.....l.....o.....p.'...r.-...s.>...t.G...v.\...w.i...y.o...z.~...|.....}.....2.....V.....\.....z..... .....E.....r.....&.....M.....;.....V.....h.....1.....+.....L.....X.....[.....j.....2.....e.....&..... E.....~.....&.....Y.....t.....O.....0.....3.....W.....x.....".....C.....U.....h.....3.....E.....D..... ".....=.....d.....e.....H.....+... .4...".I...%.....(.....*.'...+.*...,;.....k.../.....0.....1.;...3.i...4.....5.....6.x...7.....8.....9.....;.....<.0...=.U...>.....?... ..@.....A.*...C.o...D.....E...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\tr.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	425804
Entropy (8bit):	5.630152358236389
Encrypted:	false
SSDEEP:	6144:Vb44kEWcgMZ4ll7rSmilqnkdShlbh+krge5545/d+2i1TTvdzAQwiBXVx+:Vb4pMKlJe81lh+A545/T
MD5:	418DC1CDD7CCC10679523665E1626280
SHA1:	D4407BA9BC55153963150E6E30F23CC5B2304E30
SHA-256:	26FD3317BEDD4080038D7A0003D73923FC0EDD40283EF11B5BA80BB27F946C13
SHA-512:	4A907BF14DC9CD8ECB2F17152FF5EA0A6DC37034C95ED31A445395BCB9AD6FC23D4117E81F94AC82D767869B0B828738EACD33B810DF87DD41CC3EC2D5B92 E94
Malicious:	false
Preview:	.....N...h.....i.....j.....k.....l.....n.....o.....p.!...r.'...s.8...t.A...v.V...w.c...y.i...z.x...|.~...}.....!.....7.....L.....W.....e..... ....4.....;.....P.....c.....m.....\/.....?.....x.....*.....D.....\.....v..... .....4.....A.....].....l.....".....2.....D.....[.....t.....R.....\/.....=.....M.....V.....`.....i. ....p.....A.....n..... .....".....%.....(.....*.;...+.>...,.\.....s.../.....0.....1.....3.....4.....5.....6.K...7.h...8.....9.....;.....<.....=.....>.....?.....@.....A. ...C.<.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\uk.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	728668
Entropy (8bit):	4.8790394136747866
Encrypted:	false
SSDEEP:	12288:XdGPBo+VgnayTBVsFQifnSo75uB3lj5A9mERrEusLNiXElqBkyC:tGFV6cr5/E+
MD5:	0ED34D4A274D21D3376CA37DF97B3017
SHA1:	3DB12DCC6D1E85D4A497E4CB1CC8103F4A9565BE
SHA-256:	0523B68C3320674D1565DEDAF0436EC821A7175A34AC673338D6447AAB20FD7A

SHA-512:	6A5F4C02A23CABC79EC69738778A6C62685CDBE0D8CBECCD830CD75911E00CAAC4E1D0A1A2165F4CEC070E7C417D0AD13E03FE5D7E89C3352E6F2D25CB6E 2F06
Malicious:	false
Preview:	.....t.h.....i.....j.....k.....l.....n.....o.$...p.1...r.7...s.H...t.Q...v.f...w.s...y.y...z.....\|.....}.....G.....d.....}.....'.....j..... .....+.....=.....V.....j.....N.....o.....{.....7.....c.....m.....}.....3.....l.....(.....0.....>.....]..... .....8.....K.....:.....Q.....q.....1.....S.....i.....u..... .....Q.....+.....J.....^... ..r.....c.....$.....O.....a.....u..... ....."....%.P...(....*.....+.....,.....<.../.j...0.|...1.....3.....4.2...5.a...6.....7.....8.....9.(...;-...<.E...=.Y...>.....?.....@. ....A.S...C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\ur.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	637231
Entropy (8bit):	5.148107468795065
Encrypted:	false
SSDEEP:	12288:9lhG4V8PzqSMeyeSD7J/5TZPEHbWC8cQYrUu7co/9NjjFpv/j:9Lz4a5mW2
MD5:	8D6FA97205A1D2B371A54144AEA453CA
SHA1:	11A77318F571D15DAF7AD047B06E1EC8A51C8F8C
SHA-256:	578AEF61FC8B5C2E0F3765B1487F8AF9F72F6506050D501FEC9EDCBF93C7A3E4
SHA-512:	9C8DBF1126B97BCA195C801B81AFDBD8F68E8F44EBD57C563D63F6C1A3F7FA08B1ABC76E25A28D1EB2CD8BC47C9438F23B72063F081F0BCE6B8F48BD90A56 433
Malicious:	false
Preview:	.....1.h.f...i.n...j.z...k.....l.....n.....o.....p.....r.....s.....t.....v.....w.....y.....z.....|.....}.....%.....*.....2.....:.....B.....I.....P.....W.....X.....Y.....^.....$.....0.....A.....l.....x..... .....:.....`.....u.....-.....l.....o.....3.....!.....'.....*.....6.....^.....E.....t..... .....1.....?.....i.....*.....2.....5.....L.....g.....Q.....+.....?.....j..... .....6.....m.....#.....p..... .....".....%.c...(.....*.....+.....,...../.....0.1...1.~...3.....4.....5.....6.P...7.....8.....9.....;.....<.....=.....>.%...?.2...@.T... A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\vi.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	504139
Entropy (8bit):	5.815093203386653
Encrypted:	false
SSDEEP:	12288:fo4e5En2DYpgsHB30XBfwSPSoC39XPSw508ELDg4iW+U9Hzi8Bhf:w4e5ipgsHd0X9wS9e9b508wDHiW+U9TP
MD5:	7B2CBB79992021E2FA2714AE9CDF0728
SHA1:	A543C9B6D4DABD48C6B5D995CFA3C915A2B76433
SHA-256:	326E44C27579796E4B55CC281C3E4C9BF5AD7AA87156530709CD6296350758AF
SHA-512:	5C77C2DD9E5EE9D381A2524C733D3FFB55146160393BF919ED8855781D1E8ED0C4D707BD71554D7868FF53BC546344A415E846DC15F68F0E7630D49A94F1404
Malicious:	false
Preview:	.....~.h.....i.....j.....k.....l.....n.....o.....p.&...r.,...s.=...t.F...v.[...w.h...y.n...z.}...|.....}.....A.....N.....W.....~..... .....A.....K.....b.....4.....8.....=.....N.....`.....p.....1.....G.....r..... .....$.....L.....V.....u.....X.....5.....S.....c.....{.....W.....F.....Q..... a.....l.....w.....N.....f.....(... .4..."..M...%.s...(.....*.....+.....,...../.....0.%...1.Y...3.f...4.....5.....6.....7.....8.....9.,...;.=...<.G...=.X. ..>.s...?.....@.....A.....C...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\zh-CN.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	365940
Entropy (8bit):	6.683312385277625
Encrypted:	false
SSDEEP:	6144:lq8Dy2yBz8a8s7H+vlKVClmk3955CuKNP++DfIlX:lq8WfqaV+vlKVCld55JKNP++a
MD5:	D15FA5C75A835983AF2663466B5A8494
SHA1:	6580F7C91E31491A296A039F681C93810281717C
SHA-256:	B33B23552F8F76AA43671556676298C0AF54641E9F1DE27A8208750148E737CA
SHA-512:	39A63DB44E1E2B67B1937AF803336B221BBE94D3BB31B2117530886FB9E66131EFD0EB3969C251D2EE264A7C07BDAECAC330C97B1CBE74B3988CAC6FF86F3E E5
Malicious:	false

Preview:	.....h.r...i.z...j.}...k.....l.....m.....o.....p.....r.....s.....t.....v.....w.....|.....}.....#.....2.....7.....?.....F.....M.....O.....T.....%.....'... ..+.....V.....k.....(.....4.....@.....X.....d.....l.....9.....Q.....i..... .....).....5.....D.....\.....}.....(.....:.....N.....b.....q.....x.....{.....}.....0.....].....c..... .....#.....5.....G....._.....'.....;.....D... .J..".V...%.q...(.....*.....+.....,...../.....0.....1.....3.?...4.T...5.u...6.....7.....8.....9.....;.....<.....=.,...>.K...?.[...@. s...A.....C.....D...

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\locales\zh-TW.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	361711
Entropy (8bit):	6.700067542410215
Encrypted:	false
SSDEEP:	6144:guDHX49O+9vE+J8RCV2qLulexKuhz050wzqCBxBZ/9yGTm:g6Ih9OchxKuhz050wzJd/q
MD5:	C1C8F601F2D0BB06B49D870C80904907
SHA1:	6237DF5D4580AFCCAA6A07F35729F9E2737C82A8
SHA-256:	69D888BE9D5AFFC6086E901CF52936477101374ABD8186F8E8F6CC38AF826691
SHA-512:	2D68F116CBFC77A17B9FB550ADDBDE95CA09F10CE1745D5AACBB9E76DD4D041D6DE8E423844266711C64FC6733BB805311A5C8838F576D049340F32D4E0EC B2
Malicious:	false
Preview:	.....{...h.,...i.=...j.A...k.P...l.[...n.c...o.h...p.p...r.v...s.....t.....v.....w.....y.....z.....|.....}.....P.....Y.....e.....t.....z..... .....3.....B.....Z.....`.....l.....{.....D.....V.....\.....e.....q.....}..... .....&.....0.....@.....m.....0.....Q.....].....i.....o.....{... .....0.....W.....f.....l.....r.....~..... ....A.....C.....D.$.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\resources.pak

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	5193850
Entropy (8bit):	**7.9952704707488165**
Encrypted:	**true**
SSDEEP:	98304:qg1zetaMcKWPxgWMp1W/ywNAWsh11fHcMtyrwr+oxPf0yO1WODHxSkLyz7ai6y:qgVetWxWF1pkshH8M4krFPf0FIG27sy
MD5:	043DBE3EAF0BDE424185A3843E321F83
SHA1:	580AC5FDE14E6D177D6F45D2E40D435CC7EDC8D0
SHA-256:	0C967CB604D5066F1AB609E81895C1271475A2E1B4B3D5930EEA720FC218781B
SHA-512:	44814AAEC681922594528D0ED1A4D2E935045220D09E065647B53455931EAEB3B737C87032B611D7EAD621379AE653A9C5D6D87C828C1961C54129124234EBC3
Malicious:	false
Preview:	.....f.....).....+....b/...8.A...8.J...8.M...8.`...8-i...8Hp...8.r...8-y...8.{...80}...8s....8e....8.....8.....8....8+....8W....8)....8....8.....8|....8.....8;....8H....8.....8.....8y....8o....8z....8 .....8.....8^....8.....9.....9.....9.....99....9.....9.....9\"...9.B...9kD...9.I...9.S...9.U...9.V...9|W...9.Z...9.Z...9R[...9.`...9.f...9.w...9.....9x....9.....@.....@.....@....@.....@.....@.....@... ..@`....@&....@.....@.....@.....@....8E....9EB...:EV...;E....<E."..=Eu-..>E....?E./..@E.0..AEQH..BEL....FSD...F.G...U4....UH....U/....U.....U.....U....U.....U5....U.....U.....U.... .U.....U6....U.....U.....U.....U.....U.....U.....U.....VM....V^....V.....V.!...V.+...VJ2...V0A...V.D...V.J...Vi]...V.e...V.j...VK~...V....V.....Vn..."V....#Ve...$V,...%V....&V....'V(...(V... .)V....*V>...+V@....W.....WUP...W}T.....Y.....Y.....C.....y.....y.....j.....6N.....V....L^....Rc....$e....Dj.....o....1w.....-.....-...../....0.....2.....3.....4.....5.4.

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\resources\app.asar

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	21753381
Entropy (8bit):	5.860076103068824
Encrypted:	false
SSDEEP:	98304:4C74XVBntKRiyBdu6gtP6rvTAjAUoD3yWN8eVwgbA4eALFDIoZGcjy4nOsDhJZTn:H4zn1NtP6khKhkCLeR6
MD5:	72EFD30991B8146BD6A4F97425878001
SHA1:	A1378ECE6956285FEBE5DF15F9E927DE474CE66D
SHA-256:	97DB379B5529C330D80FE9E6EA4C189D88A651527D9274A32176B494E2ADFD96
SHA-512:	4C0D4C5C3633F2278F5CB38769DC60BCD8DE5171CB1C2E1346A8ED47C080252D30C4110606E3C2D12F1DFF11172DAB8E48C9D12649F699580D6B53DB4AFED C
Malicious:	false

Preview:	.....{"files":{"icon.ico":{"size":20849,"integrity":{"algorithm":"SHA256","hash":"6b69fa073c3e7fdbcb22c727e6935453a0aa3407e302c2d917f9a8666b8abd1a","blockSize":4194304,"blocks":["6b69fa073c3e7fdbcb22c727e6935453a0aa3407e302c2d917f9a8666b8abd1a"]},"offset":"0"},"index.js":{"size":1011233,"integrity":{"algorithm":"SHA256","hash":"1910d8b7709e95c7ac67836126d5d782d05d1881398b66d6d7b769b1a9f980fe","blockSize":4194304,"blocks":["1910d8b7709e95c7ac67836126d5d782d05d1881398b66d6d7b769b1a9f980fe"]},"offset":"20849"},"package.json":{"size":506,"integrity":{"algorithm":"SHA256","hash":"396ea2c9f9490938ec21ef6faf4cba0fac6b16b2ef267e204567503c8bf15ee6","blockSize":4194304,"blocks":["396ea2c9f9490938ec21ef6faf4cba0fac6b16b2ef267e204567503c8bf15ee6"]},"offset":"1032082"},"node_modules":{"files":{"asynckit":{"files":{"LICENSE":{"size":1078,"integrity":{"algorithm":"SHA256","hash":"1953150d5d4b10c7542cee6f6e0c613b2682545233f069d75cfff1936386ce10","blockSize":4194304,"blocks":["1953150d5d4b10

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\resources\elevate.exe

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107520
Entropy (8bit):	6.442687067441468
Encrypted:	false
SSDEEP:	3072:1bLnrwQoRDtdMMgSXiFJWcIgUVCfRjV/GrWl:1PrwRhte1XsE1l
MD5:	792B92C8AD13C46F27C7CED0810694DF
SHA1:	D8D449B92DE20A57DF722DF46435BA4553ECC802
SHA-256:	9B1FBF0C11C520AE714AF8AA9AF12CFD48503EEDECD7398D8992EE94D1B4DC37
SHA-512:	6C247254DC18ED81213A978CCE2E321D6692848C64307097D2C43432A42F4F4F6D3CF22FB92610DFA8B7B16A5F1D94E9017CF64F88F2D08E79C0FE71A9121E4(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..O.....h.....j.q.....k.....e.....e.....e.....zR....._....h.... ..h.f.....h.....Rich.....PE..L.....W.....l.....0....@.....@.....P.....x.....T.....p..... .....@.....0..$.....text..... ..`.rdata...k...0...l.....@..@.data.....@....gfids.....@..@.rsrc...x..... .....@..@.reloc..T.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\snapshot_blob.bin

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	259202
Entropy (8bit):	4.177720672914121
Encrypted:	false
SSDEEP:	1536:N8eVec2PhNMqkPhmpILx3FtscrrDKrVTT9gXA4SuoveydoBaDEtu/wMHOdxpMKrF:76N6PkpILxHscrXeQZb0G0mvY6T
MD5:	3A4095538E021B84396B3CE25AFFAFC3
SHA1:	CFC20771227B3C1F3197FF6A91CEE68555AFB247
SHA-256:	C1C9145735032BFF20B2FFF50A4B92AE9CF47290F433E3F3B32E3B232D610C59
SHA-512:	7B71083180F237F5F37CBE7A9755F6606708B959986562F9C5880CCCEA17B80A5187649FC0CB6965A8B40526BCB2CB6D980D364BE528465290658B4D9084348E
Malicious:	false
Preview:	.....J.&11.4.183.29-electron.0.....h...B%...Y.....a.....a.....a.....ar.....a.....a.....].D.....M....`$.....m.D.....=....`$.....D.....M....`$. .....u.D.....M....`$.....D.....A....`D.....D.....M....`$.....M.D.....M....`$.....D.....M....`$.....D.!....M....`$.....q.D.%.....E....`$.....D.)....M....`$.....ID.-.....M....`$... ....D.1.....M....`$.....D.5.....M....`$....(Jb...(L.....@..F^.....`.....(Jb...,P.....@..F^..`.....H...IDa.....Db.....D`.....D`.....D]D....D`.....Wla.....Wla.....Wla.....Wla.... .....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....L..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\v8_context_snapshot.bin

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	data
Category:	dropped
Size (bytes):	578034
Entropy (8bit):	5.245532016724801
Encrypted:	false
SSDEEP:	6144:alKQ1+Ku6X5O8QgZbNg8zvEjbwTBH32jezyjPX:aV1oeLvs4mCG
MD5:	5DB8A5BB87C7999343F30128979057A1
SHA1:	C4177C2FE973A495DB59B6228AC26264EEC46A4D
SHA-256:	5B1F69F39F3D5865DCE13EE3BDBC1AF2938F5CC4C056DC9F9E213E9AF346AD4B
SHA-512:	DA2D516251376952729A33DE2CD23764290D400FAFC49642F2CCD799E3F989CCE4D5561A76D380A950B77B53B50148DEC9089C30DE6C3DC38666237E196E569
Malicious:	false

Preview:	..... .R.11.4.183.29-electron.0.....p.....*....y.....@p..a.....a.....aT.....ar.....a.....a.....].D.....M....`$.....m.D.....=....`$.....D.....M ....`$.....u.D.....M....`$.....D.....A....`D.....D.....M....`$.....M.D.....M....`$.....D.....M....`$.....D.!....M....`$.....q.D.%....E....`$.....D.)....M....`$.....ID.-.....M....`$..... .D.1.....M....`$.....D.5.....M....`$....(Jb...(L.....@..F^.....`.....(Jb...,P.....@..F^..`.....H...IDa.....Db.....D`.....D`.....D]D....D`.....Wla.....Wla.....Wla.....Wla..... ....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....Wla.....L..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\vk_swiftshader.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5251072
Entropy (8bit):	6.341324832913826
Encrypted:	false
SSDEEP:	49152:Ab03fn3GIdr1DO1N8jvfWSrvOuyEE0+w7rz77gpxbhk0H4t38mvttDpSHUoeygs4:d3v3xDvRTGVgt38mvt1pSH0adU
MD5:	516C5B93B1C13AF0AD393BFF6AA4E259
SHA1:	A8823263EE4C2B7CED5AEA055E6F4105DF09E478
SHA-256:	2377FD655C1E0B6275F109258F3AF70161996F6CCBF8D67BB654D3A9EDF6D5B9
SHA-512:	B976C2373525DD1AC9493D281EC5A1685D1C63B41C44DB6F0DF10915A6C97A2E041D3F00485AADF7B52695C901D5AB1FE2FFE0CAA7AEEAE6874065B185D81A 22
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke....." .....?..z.....9.....Q.....`A.... .....zK.~...f.K.P.....Q.....@O..`..... Q.h}...8K.....7K.(...@.?.@.....K.P.....text.....?.....?..... ..`.rdata.....?.....?... .....@..@.data.....L.....pL.....@....pdata...`...@O..`....N.....@..@.00cfg..8.....P.....fO.....@..@.gxfg.....,....P.....hO.....@..@.retplne.....P.....O... .....tls....Q.....P.....O.....@..._RDATA..\.....Q.....O.....@..@.rsrc.....Q.....O.....@..@.reloc..h}... Q..~....O.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\vk_swiftshader_icd.json

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	4.724752649036734
Encrypted:	false
SSDEEP:	3:YD96WyV18tzsmyXLVi1rTVWSCwW2TJHzeZ18rY:Y8WyV18tAZLVmCwXFiZ18rY
MD5:	8642DD3A87E2DE6E991FAE08458E302B
SHA1:	9C06735C31CEC00600FD763A92F8112D085BD12A
SHA-256:	32D83FF113FEF532A9F97E0D2831F8656628AB1C99E9060F0332B1532839AFD9
SHA-512:	F5D37D1B45B006161E4CEFEEBBA1E33AF879A3A51D16EE3FF8C3968C0C36BBAFAE379BF9124C13310B77774C9CBB4FA53114E83F5B48B5314132736E5BB449 6F
Malicious:	false
Preview:	{"file_format_version": "1.0.0", "ICD": {"library_path": ".\\vk_swiftshader.dll", "api_version": "1.0.5"}}

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\7z-out\vulkan-1.dll

Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	931840
Entropy (8bit):	6.56671155058839
Encrypted:	false
SSDEEP:	24576:FoHDVVdrfQ09CPKuy0O0Q6Z5W0DYsHA6g3P0zAk7m+:FuVdrI0GKuy066Z5W0DYsHA6g3P0zAk5
MD5:	D1F1609B93993A1C74872FAF7694B01D
SHA1:	4237815549B77F3509EE99F8ED6A86DE6C15AA20
SHA-256:	D0615DC92873F5FC92A74CDED1E0EC34A702D6A3E671778C841BE20DA2CD4549
SHA-512:	CD80B50476C4358E06736789B99C5F8C97F3FA5C7DEE85610EED26A5EA42189F6475F97FF00B7D11C15DBE72B9B7734EB01732275A1B510D13663DC775EFF81
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...l.Ke....." .....x.....`A.... .....0...<!..l...P.....o.....L...<..... ...(...@...@.....text....v.....x..... ..`.rdata.....\|..... @..@.data....L..... ...d.....@....pdata...o.....p.....@..@.00cfg..8....@.....@..@.gxfg...P(...P...*.....@..@.retplne..... .....tls.. .....".....@..._RDATA..\.....$.....@..@.rsrc.....&.....@..@.reloc..L.....*.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\SpiderBanner.dll	
Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	5.5347224014600345
Encrypted:	false
SSDEEP:	192:5lkE3uqRI1y7/xcfK4PRef6gQzJyY1rpKIVrw:5lkMBI1y7UKcef6XzJrpKY
MD5:	17309E33B596BA3A5693B4D3E85CF8D7
SHA1:	7D361836CF53DF42021C7F2B148AEC9458818C01
SHA-256:	996A259E53CA18B89EC36D038C40148957C978C0FD600A268497D4C92F882A93
SHA-512:	1ABAC3CE4F2D5E4A635162E16CF9125E059BA1539F70086C2D71CD00D41A6E2A54D468E6F37792E55A822D7082FB388B8DFECC79B59226BBB047B7D28D44D28
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.../../../..Wy./../../...../..Wi./..Wx./..W~./..W{./..Rich./.....PE..L...T{mW.....!.....p!.....0.....p.....@.....5..o...I1..P....P.....`.....0.....text..... ..`.rdata.....0.....@..@.data.....@.....@....rsrc.....P.....@..@.reloc..d...`..... .....@..B.....

C:\Users\user\AppData\Local\Temp\nsr97EA.tmp\StdUtils.dll	
Process:	C:\Users\user\Desktop\WolferVPN.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	102400
Entropy (8bit):	6.729923587623207
Encrypted:	false
SSDEEP:	3072:WNuZmJ9TDP3ahD2TF7Rq9cJNPhF9vyHf:WNuZ81zaAFHhF9v
MD5:	C6A6E03F77C313B267498515488C5740
SHA1:	3D49FC2784B9450962ED6B82B46E9C3C957D7C15
SHA-256:	B72E9013A6204E9F01076DC38DABBF30870D44DFC66962ADBF73619D4331601E
SHA-512:	9870C5879F7B72836805088079AD5BBAFCB59FC3D9127F2160D4EC3D6E88D3CC8EBE5A9F5D20A4720FE6407C1336EF10F33B2B9621BC587E930D4CBACF33783
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q....C...C...C...C...C...C...C...C...C...C...C...C.[.C...C.[.C...C.[.C...C.[.C...CRich...C.....PE..L...I..[.....!.....*...b.....@.....+....@.....}..d....t.....X.....@.....text....).....*..... ..`.rdata..TC...@...D.....@..@.data...I.....r.....@....rsrc...X.....x.....@..@.reloc..j.....~.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.999984252619177
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:	WolferVPN.exe
File size:	74'280'552 bytes
MD5:	6434ceafa88a3afa1f8351bc6890b2a5
SHA1:	700b43db6881bc83c6d7acb0d020283dca4fa7ba
SHA256:	db230e271893be37515e7bf1403352d99a5f8ac441c2df589551ee399dea7315
SHA512:	d61648811d069b6b973c234b391704ac6bc714d808f48afff5a5c39705b320cb0cc8091e6c54d18368a8b0a4187fbb0f2444f99262121145d80281bf28b9ef6a
SSDEEP:	1572864:5MpHvAncNj5mA99v/X6s/WXct35tOfMIGKID0aJvi67YoKEiakmB25:5+GcNF99Jys/WXOJtOfMIGKIwsUAhy
TLSH:	15F73309C7C66311FB848BB9A59A7317D589F238EF8022643075831E3876FEFAD69507
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....\.....h...8...@.

File Icon

Icon Hash:	1739cd9f92613386

Static PE Info

General

Entrypoint:	0x40338f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5C157F86 [Sat Dec 15 22:26:14 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	b34f154ec913d2d2c435cbd644e91687

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0047AEECh], eax
je 00007F75F87CE5D3h
push ebx
call 00007F75F87D1885h
cmp eax, ebx
je 00007F75F87CE5C9h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F75F87D17FFh
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h

Instruction
jne 00007F75F87CE5ACh
push 0000000Ah
call 00007F75F87D1858h
push 00000008h
call 00007F75F87D1851h
push 00000006h
mov dword ptr [0047AEE4h], eax
call 00007F75F87D1845h
cmp eax, ebx
je 00007F75F87CE5D1h
push 0000001Eh
call eax
test eax, eax
je 00007F75F87CE5C9h
or byte ptr [0047AEEFh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [0047AFB8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 00440208h
call dword ptr [00408188h]
push 0040A2C8h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19f000	0x7330	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6627	0x6800	False	0.6646259014423077	data	6.450282348506287	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a2	0x1600	False	0.4405184659090909	data	5.025178929113415	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	0xa000	0x70ff8	0x600	False	0.5182291666666666	data	4.037117731448378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x7b000	0x124000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x19f000	0x7330	0x7400	False	0.7661974676724138	data	7.150293516996489	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x19f4a8	0x515b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States	0.9935180294809622
RT_DIALOG	0x1a4608	0x202	data	English	United States	0.4085603112840467
RT_DIALOG	0x1a4810	0xf8	data	English	United States	0.6290322580645161
RT_DIALOG	0x1a4908	0xee	data	English	United States	0.6260504201680672
RT_DIALOG	0x1a49f8	0x1fa	data	English	United States	0.40118577075098816
RT_DIALOG	0x1a4bf8	0xf0	data	English	United States	0.6666666666666666
RT_DIALOG	0x1a4ce8	0xe6	data	English	United States	0.6565217391304348
RT_DIALOG	0x1a4dd0	0x1ee	data	English	United States	0.38866396761133604
RT_DIALOG	0x1a4fc0	0xe4	data	English	United States	0.6447368421052632
RT_DIALOG	0x1a50a8	0xda	data	English	United States	0.6422018348623854
RT_DIALOG	0x1a5188	0x1ee	data	English	United States	0.3866396761133603
RT_DIALOG	0x1a5378	0xe4	data	English	United States	0.6359649122807017
RT_DIALOG	0x1a5460	0xda	data	English	United States	0.6376146788990825
RT_DIALOG	0x1a5540	0x1f2	data	English	United States	0.39759036144578314
RT_DIALOG	0x1a5738	0xe8	data	English	United States	0.6508620689655172
RT_DIALOG	0x1a5820	0xde	data	English	United States	0.6486486486486487
RT_DIALOG	0x1a5900	0x202	data	English	United States	0.42217898832684825
RT_DIALOG	0x1a5b08	0xf8	data	English	United States	0.6653225806451613
RT_DIALOG	0x1a5c00	0xee	data	English	United States	0.6512605042016807
RT_GROUP_ICON	0x1a5cf0	0x14	data	English	United States	1.05
RT_VERSION	0x1a5d08	0x1fc	data	English	United States	0.5039370078740157
RT_MANIFEST	0x1a5f08	0x423	XML 1.0 document, ASCII text, with very long lines (1059), with no line terminators	English	United States	0.5127478753541076

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW

DLL	Import
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 2, 2023 22:05:02.173693895 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.173713923 CET	443	49720	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.173815012 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.176538944 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.176570892 CET	443	49721	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.176649094 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.177963018 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.177983046 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.178050041 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.178590059 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.178616047 CET	443	49723	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.178699970 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.179224968 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.179260969 CET	443	49724	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.179303885 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.180560112 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.180591106 CET	443	49725	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.180639029 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.181195974 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.181222916 CET	443	49726	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.181269884 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.194216013 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.194226027 CET	443	49720	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.200684071 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.200699091 CET	443	49721	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.202045918 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.202065945 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.204683065 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.204701900 CET	443	49723	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.207865000 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.207885981 CET	443	49724	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.211738110 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.211766958 CET	443	49725	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.214864016 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.214896917 CET	443	49726	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.472959995 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.473614931 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.473637104 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.475410938 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.475508928 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.478540897 CET	443	49725	172.67.218.203	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 2, 2023 22:05:02.478873014 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.478928089 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.479074955 CET	443	49722	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.479146957 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.479146957 CET	49722	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.481540918 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.481556892 CET	443	49725	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.482613087 CET	443	49725	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.482685089 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.483414888 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.483453989 CET	443	49725	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.483572006 CET	443	49725	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.483644962 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.483663082 CET	49725	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.520314932 CET	443	49720	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.521063089 CET	443	49721	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.521461964 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.521471977 CET	443	49720	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.521665096 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.521682024 CET	443	49721	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.522852898 CET	443	49720	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.522921085 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.523288012 CET	443	49721	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.523355961 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.523961067 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.523997068 CET	443	49720	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.524064064 CET	49720	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.528177977 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.528223038 CET	443	49721	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.528287888 CET	49721	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.531627893 CET	443	49723	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.531639099 CET	443	49724	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.532636881 CET	443	49726	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.553942919 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.553953886 CET	443	49724	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.554162025 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.554177999 CET	443	49723	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.554372072 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.554394007 CET	443	49726	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.555140018 CET	443	49724	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.555207968 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.555357933 CET	443	49723	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.555412054 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.555481911 CET	443	49726	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.555536985 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.573386908 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.573457003 CET	443	49723	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.573545933 CET	49723	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.574502945 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:02.574565887 CET	443	49726	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:02.574623108 CET	49726	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:03.689687967 CET	49728	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:03.689718962 CET	443	49728	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:03.689780951 CET	49728	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:03.690819979 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:03.690934896 CET	443	49724	172.67.218.203	192.168.2.6
Dec 2, 2023 22:05:03.691005945 CET	49724	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:03.692272902 CET	49728	443	192.168.2.6	172.67.218.203
Dec 2, 2023 22:05:03.692285061 CET	443	49728	172.67.218.203	192.168.2.6

DNS Queries

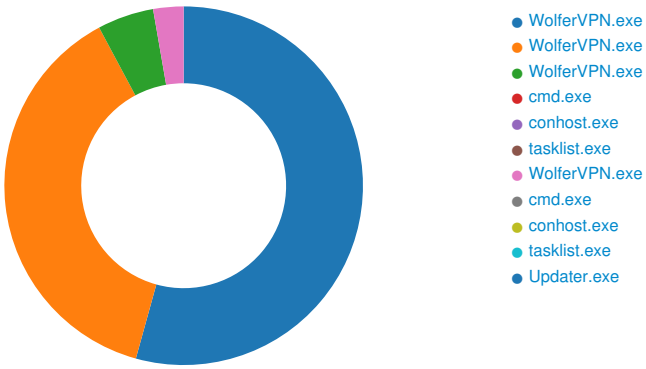
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 2, 2023 22:04:58.641046047 CET	192.168.2.6	1.1.1.1	0x40d6	Standard query (0)	rufflesref ined.com	A (IP address)	IN (0x0001)	false
Dec 2, 2023 22:05:09.658327103 CET	192.168.2.6	1.1.1.1	0x6693	Standard query (0)	chrome.clo udflare-dns.com	A (IP address)	IN (0x0001)	false
Dec 2, 2023 22:05:09.658950090 CET	192.168.2.6	1.1.1.1	0x35bb	Standard query (0)	chrome.clo udflare-dns.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 2, 2023 22:04:58.780168056 CET	1.1.1.1	192.168.2.6	0x40d6	No error (0)	rufflesref ined.com		172.67.218.203	A (IP address)	IN (0x0001)	false
Dec 2, 2023 22:04:58.780168056 CET	1.1.1.1	192.168.2.6	0x40d6	No error (0)	rufflesref ined.com		104.21.24.126	A (IP address)	IN (0x0001)	false
Dec 2, 2023 22:05:09.787301064 CET	1.1.1.1	192.168.2.6	0x6693	No error (0)	chrome.clo udflare-dns.com		172.64.41.3	A (IP address)	IN (0x0001)	false
Dec 2, 2023 22:05:09.787301064 CET	1.1.1.1	192.168.2.6	0x6693	No error (0)	chrome.clo udflare-dns.com		162.159.61.3	A (IP address)	IN (0x0001)	false
Dec 2, 2023 22:05:09.789047956 CET	1.1.1.1	192.168.2.6	0x35bb	No error (0)	chrome.clo udflare-dns.com			65	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: WolferVPN.exe PID: **1416**, Parent PID: **4004**

General

Target ID:	0
Start time:	22:04:25
Start date:	02/12/2023
Path:	C:\Users\user\Desktop\WolferVPN.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\WolferVPN.exe
Imagebase:	0x400000
File size:	74'280'552 bytes
MD5 hash:	6434CEAFA88A3AFA1F8351BC6890B2A5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	success or wait	1	406184	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	success or wait	1	406184	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	InstallLocation	unicode	C:\Users\user\AppData\Local\Programs\WolferVPN	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	KeepShortcuts	unicode	true	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	ShortcutName	unicode	WolferVPN	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	DisplayName	unicode	WolferVPN 1.0.0	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	UninstallString	unicode	"C:\Users\user\AppData\Local\Programs\WolferVPN\Uninstall WolferVPN.exe" /currentuser	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	QuietUninstallString	unicode	"C:\Users\user\AppData\Local\Programs\WolferVPN\Uninstall WolferVPN.exe" /currentuser /S	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	DisplayVersion	unicode	1.0.0	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	DisplayIcon	unicode	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe,0	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	NoModify	dword	1	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	NoRepair	dword	1	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\9c1054f2-f2ad-5af7-8c3f-0bca1902f573	EstimatedSize	dword	257056	success or wait	1	402475	RegSetValueExW

Analysis Process: WolferVPN.exe PID: **6732**, Parent PID: **4004**

General

Target ID:	5
Start time:	22:04:54
Start date:	02/12/2023
Path:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe"
Imagebase:	0x7ff65fa30000
File size:	163'343'360 bytes
MD5 hash:	4AD8066DFB8E65195E5733DDFD8A1AC7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs • Detection: 1%, Virustotal, Browse
Reputation:	low
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b1c3f10e-540e-46f8-9bee-83879b20c9f6.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF66134475F	CreateFileW
C:\Users\user\AppData\Roaming\WolferVPN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF66134652B	CreateDirectoryW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bby	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Temp\8aa2ec43-5e03-40f0-b44b-d7dcf4df059c.tmp	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF66134475F	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bby	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.bby	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data.bby	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data.bby	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FF6620C1029	CopyFileW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies.bby</td><td>read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write</td><td>device</td><td>sequential only | synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>7FF6620C1029</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe</td><td>write data or add file | append data or add subdirectory or create pipe instance | write e a | read attributes | write attributes | read control | sync hronize</td><td>device</td><td>synchronous io non alert | open for backup ident</td><td>success or wait</td><td>1</td><td>7FF6620BDD94</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\WolferVPN\70a796c8-78d6-49f5-8289-083fe8def8a7.tmp</td><td>read attributes | delete | syn chronize | generic read | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>7FF66134475F</td><td>CreateFileW</td></tr>
</table>

File Moved

<table>
<tr><th>Old File Path</th><th>New File Path</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\b1c3f10e-540e-46f8-9bee-83879b20c9f6.tmp</td><td></td><td>success or wait</td><td>1</td><td>7FF6656E221F</td><td>MoveFileExW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\8aa2ec43-5e03-40f0-b44b-d7dcf4df059c.tmp</td><td></td><td>success or wait</td><td>1</td><td>7FF6656E221F</td><td>MoveFileExW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\WolferVPN\70a796c8-78d6-49f5-8289-083fe8def8a7.tmp</td><td></td><td>success or wait</td><td>1</td><td>7FF6613450F7</td><td>MoveFileW</td></tr>
</table>

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\b1c3f10e-540e-46f8-9bee-83879b20c9f6.tmp.node</td><td>0</td><td>152576</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 fd fd 10 74 fd fd 7e 27 fd fd 7e 27 fd fd 7e 27 2f fd 7d 26 fd fd 7e 27 2f fd 7b 26 76 fd 7e 27 2f fd 7a 26 fd fd 7e 27 58 fd 7a 26 fd 7e 27 58 fd 7d 26 fd fd 7e 27 58 fd 7b 26 f8 7e 27 2f fd 7f 26 fd fd 7e 27 fd fd 7f 27 fd fd 7e 27 fd fd 77 26 fd fd 7e 27 fd c1 27 fd fd 7e 27 fd fd 7c 26 fd fd 7e 27 52 69 63 68 fd fd 7e 27 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07</td><td>MZ@!L!This program cannot be run in DOS mode.$t~'~'~'/}&~'/{&v~'/z&~'Xz&~'X}&~'X{&~'/&~''~'w&~''~'|&~'Rich~'PEd</td><td>success or wait</td><td>1</td><td>7FF661343D39</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bby	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Temp\8aa2ec43-5e03-40f0-b44b-d7dcf4df059c.tmp.node	0	1648128	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5b 61 16 0a 1f 00 78 59 1f 00 78 59 1f 00 78 59 fd 72 7b 58 0b 00 78 59 fd 72 7d 58 fd 00 78 59 fd 72 7c 58 3d 00 78 59 4d 75 7c 58 11 00 78 59 4d 75 7b 58 16 00 78 59 4d 75 7d 58 36 00 78 59 fd 72 79 58 1c 00 78 59 1f 00 79 59 fd 00 78 59 fd 75 71 58 1c 00 78 59 fd 75 78 58 1e 00 78 59 fd 75 fd 59 1e 00 78 59 fd 75 7a 58 1e 00 78 59 52 69 63 68 1f 00 78 59 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$[axYxYxYr{XxYr}XxYr|X=xYMu|XxYMu{XxYMu}X6xYr yXxYyYxYuqXxYuxXxYuYxYuzXxYRichxY	success or wait	1	7FF661343D39	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bby	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.bby	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	7FF6620C1029	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data.bby	0	51200	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 05 00 00 00 02 07 fd 00 00 00 00 18 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data.bby	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 08 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 37 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y7.jW	success or wait	2	7FF6620C1029	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies.bby	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 0d 0d 24 00 04 0a 0c 00 0f 67 0f fd 0a 0c 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j$g	success or wait	1	7FF6620C1029	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe	0	65536	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 fd 0f 00 6c fd 4b 65 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 00 00 fd fd 07 00 66 fd 01 00 00 00 00 fd 6a 25 04 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd fd 09 00 04 00 00 00 00 00 00 02 00 60 fd 00 00 fd 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEdlKe"fj%@`	success or wait	2493	7FF6620BF0AB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WolferVPN\70a796c8-78d6-49f5-8289-083fe8def8a7.tmp	0	413	7b 22 6f 73 5f 63 72 79 70 74 22 3a 7b 22 65 6e 63 72 79 70 74 65 64 5f 6b 65 79 22 3a 22 52 46 42 42 55 45 6b 42 41 41 41 41 30 49 79 64 33 77 45 56 30 52 47 4d 65 67 44 41 54 38 4b 58 36 77 45 41 41 41 42 53 6a 4c 55 37 7a 59 55 6b 52 49 50 44 52 33 49 4b 43 55 45 59 45 41 41 41 41 42 49 41 41 42 44 41 47 67 41 63 67 42 76 41 47 30 41 61 51 42 31 41 47 30 41 41 41 41 51 5a 67 41 41 41 41 45 41 41 43 41 41 41 41 41 65 4d 61 50 64 71 76 55 33 58 62 69 30 54 30 32 5a 48 35 77 74 44 36 41 4a 57 38 41 6c 4f 56 46 37 53 47 74 32 35 37 64 4a 69 41 41 41 41 41 41 4f 67 41 41 41 41 41 49 41 41 43 41 41 41 41 43 72 4c 38 35 63 39 75 36 49 69 6a 50 74 39 31 78 6c 70 55 63 39 72 78 53 61 5a 36 66 6c 69 4c 4c 52 76 42 39 45 33 77 46 59 54 41 41 41 41 43 41 4c	{"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABSjLU7zYUkRIPDR3IKCUEYEAAAABIAAABDAGgAcgBvAG0AaQB1AG0AAAAQZgAAAAEAACAAAAAeMaPdqvU3Xbi0T02ZH5wtD6AJW8AlOVF7SGt257dJiAAAAAAOgAAAAIAACAAAACrL85c9u6IBijPt91xlpUc9rxSaZ6fliLLRvB9E3wFYTAAAACAL

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bby	0	2048	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bby	0	100	success or wait	2	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bby	0	2048	success or wait	2	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.bby	0	100	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.bby	0	4096	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	44455	success or wait	1	7FF6620BE9D7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data.bby	0	100	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data.bby	0	2048	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data.bby	0	100	success or wait	2	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Web Data.bby	0	2048	success or wait	2	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies.bby	0	100	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies.bby	0	4096	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\key4.db	unknown	294912	success or wait	1	7FF6620BE9D7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cookies.sqlite	0	100	success or wait	1	7FFD9404B556	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\2o7hffxt.default-release\cookies.sqlite	0	32768	success or wait	2	7FFD9404B556	ReadFile
\pipe\uv\0000000000000000-6732	0	0	pending	1	7FF6620D16C5	ReadFile
\pipe\uv\0000000000000001-6732	0	0	pending	1	7FF6620D16C5	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	pending	1	7FF65FE9CF4C	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	success or wait	4	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	success or wait	5	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	pending	4	7FF66310B184	ReadFile
\pipe\uv\0000000000000000-6732	unknown	65536	success or wait	1988	7FF6620D246E	ReadFile
\pipe\uv\0000000000000000-6732	0	0	pending	1930	7FF6620D16C5	ReadFile
\pipe\uv\0000000000000000-6732	0	0	success or wait	58	7FF6620D16C5	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	unknown	8192	end of file	1	7FF6620BE9D7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\000003.log	unknown	8192	end of file	1	7FF6620BE9D7	ReadFile
C:\Windows\System32\spool\drivers\color\sRGB Color Space Profile.icm	unknown	4096	success or wait	1	7FF663CA56F9	ReadFile
C:\Windows\System32\spool\drivers\color\sRGB Color Space Profile.icm	unknown	4096	end of file	1	7FF663CA56F9	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe	unknown	65536	success or wait	1466	7FF6620BE9D7	ReadFile
\pipe\uv\0000000000000000-6732	0	0	pending	1	7FF6620D16C5	ReadFile
\pipe\uv\0000000000000001-6732	0	0	pending	1	7FF6620D16C5	ReadFile
\pipe\uv\0000000000000000-6732	unknown	65536	success or wait	2022	7FF6620D246E	ReadFile
\pipe\uv\0000000000000000-6732	0	0	pending	1813	7FF6620D16C5	ReadFile
\pipe\uv\0000000000000000-6732	0	0	success or wait	209	7FF6620D16C5	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe	unknown	65536	end of file	1	7FF6620BE9D7	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	pending	1	7FF65FE9CF4C	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	success or wait	2	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	pending	3	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	pending	6	7FF66310B184	ReadFile

Analysis Process: WolferVPN.exe PID: **2328**, Parent PID: **6732**

General

Target ID:	9
Start time:	22:04:56
Start date:	02/12/2023
Path:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe" --type=gpu-process --user-data-dir="C:\Users\user\AppData\Roaming\WolferVPN" --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=1680 --field-trial-handle=1684,i,1620382105047154044,16004179749874181730,262144 --disable-features=SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand /prefetch:2
Imagebase:	0x7ff65fa30000
File size:	163'343'360 bytes
MD5 hash:	4AD8066DFB8E65195E5733DDFD8A1AC7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	success or wait	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	end of file	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	512	success or wait	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	success or wait	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	end of file	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	success or wait	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	end of file	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	success or wait	1	7FFD92CC4079	ReadFile
C:\Users\user\AppData\Local\Programs\WolferVPN\vk_swiftshader_icd.json	unknown	4096	end of file	1	7FFD92CC4079	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	success or wait	1	7FF65FE9CF4C	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	pending	4	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	success or wait	2	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.12386037009875924395	0	4096	pending	5	7FF66310B184	ReadFile

Analysis Process: cmd.exe PID: **7072**, Parent PID: **6732**

General

Target ID:	10
Start time:	22:04:58
Start date:	02/12/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /d /s /c "tasklist"
Imagebase:	0x7ff7d1270000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1224**, Parent PID: **7072**

General

Target ID:	11
Start time:	22:04:59
Start date:	02/12/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: tasklist.exe PID: **2708**, Parent PID: **7072**

General

Target ID:	12
Start time:	22:05:00
Start date:	02/12/2023
Path:	C:\Windows\System32\tasklist.exe
Wow64 process (32bit):	false
Commandline:	tasklist
Imagebase:	0x7ff714ba0000
File size:	106'496 bytes
MD5 hash:	D0A49A170E13D7F6AEBBEFED9DF88AAA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: WolferVPN.exe PID: **1616**, Parent PID: **6732**

General

Target ID:	13
Start time:	22:05:01
Start date:	02/12/2023
Path:	C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Programs\WolferVPN\WolferVPN.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --user-data-dir="C:\Users\user\AppData\Roaming\WolferVPN" --mojo-platform-channel-handle=2204 --field-trial-handle=1684,i,16203821050 47154044,16004179749874181730,262144 --disable-features=SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand /prefetch:8
Imagebase:	0x7ff65fa30000

File size:	163'343'360 bytes
MD5 hash:	4AD8066DFB8E65195E5733DDFD8A1AC7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\mojo.6732.5532.18326803518997075824	0	4096	success or wait	1	7FF65FE9CF4C	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	pending	3	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	pending	3	7FF66310B184	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	4096	success or wait	2	7FF66310B184	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	4096	success or wait	1	7FF663CA56F9	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	4096	end of file	1	7FF663CA56F9	ReadFile
\pipe\mojo.6732.5532.18326803518997075824	0	56	success or wait	1	7FF66310B184	ReadFile

Analysis Process: cmd.exe PID: **6536**, Parent PID: **6732**

General

Target ID:	14
Start time:	22:05:01
Start date:	02/12/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /d /s /c "tasklist"
Imagebase:	0x7ff7d1270000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: conhost.exe PID: **936**, Parent PID: **6536**

General

Target ID:	15
Start time:	22:05:01
Start date:	02/12/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff66e660000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: tasklist.exe PID: **4800**, Parent PID: **6536**

General	
Target ID:	16
Start time:	22:05:01
Start date:	02/12/2023
Path:	C:\Windows\System32\tasklist.exe
Wow64 process (32bit):	false
Commandline:	tasklist
Imagebase:	0x7ff714ba0000
File size:	106'496 bytes
MD5 hash:	D0A49A170E13D7F6AEBBEFED9DF88AAA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: Updater.exe PID: **1948**, Parent PID: **4004**

General	
Target ID:	17
Start time:	22:05:10
Start date:	02/12/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe"
Imagebase:	0x7ff6b7400000
File size:	163'343'360 bytes
MD5 hash:	4AD8066DFB8E65195E5733DDFD8A1AC7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low
Has exited:	false

Disassembly

No disassembly