ID: 352258
Sample Name: via-1.3.1-win.exe
Cookbook: default.jbs
Time: 05:32:18
Date: 12/02/2021
Version: 31.0.0 Emerald

Table of Contents

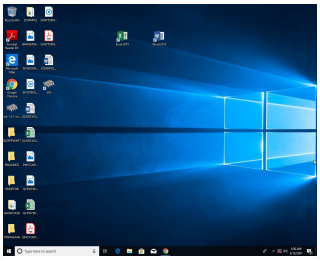
Analysis Report via-1.3.1-win.exe

Overview

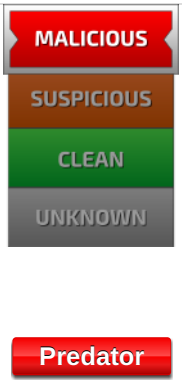
General Information

Sample Name:	via-1.3.1-win.exe
Analysis ID:	352258
MD5:	19a1e8ac63bd56..
SHA1:	f36527732732441.
SHA256:	4258ba2302fa848.

Most interesting Screenshot:



Detection

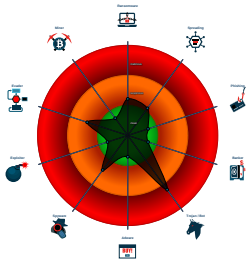


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Predator
- Contains capabilities to detect virtua…
- Contains functionality for read data f…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to shutdown / …
- Creates a process in suspended mo…
- Detected potential crypto function
- Drops PE files
- Enables security privileges
- Found dropped PE file which has no…
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- via-1.3.1-win.exe (PID: 4084 cmdline: 'C:\Users\user\Desktop\via-1.3.1-win.exe' MD5: 19A1E8AC63BD56062B2E9F0E98AE2B5E)
- VIA.exe (PID: 6868 cmdline: 'C:\Users\user\AppData\Local\Programs\via\VIA.exe' MD5: 0474F56BEB38D2AF8C20BB44D66CEBCA)
  - VIA.exe (PID: 6376 cmdline: 'C:\Users\user\AppData\Local\Programs\via\VIA.exe' --type=gpu-process --field-trial-handle=1588,13949046230613957204,7885526779198411413,131072 --disable-features=SpareRendererForSitePerProcess --gpu-preferences=KAAAAAAAAADgAAAwAAAAAAAAAYAAAAAAAEAAAAAAAAAAAAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --service-request-channel-token=10484998783080688572 --mojo-platform-channel-handle=1604 --ignored=' --type=renderer ' /prefetch:2 MD5: 0474F56BEB38D2AF8C20BB44D66CEBCA)
  - VIA.exe (PID: 6408 cmdline: 'C:\Users\user\AppData\Local\Programs\via\VIA.exe' --type=utility --field-trial-handle=1588,13949046230613957204,78855267791981141 3,131072 --disable-features=SpareRendererForSitePerProcess --lang=en-US --service-sandbox-type=network --service-request-channel-token=3061075516634477466 --mojo-platform-channel-handle=1928 /prefetch:8 MD5: 0474F56BEB38D2AF8C20BB44D66CEBCA)
  - VIA.exe (PID: 4788 cmdline: 'C:\Users\user\AppData\Local\Programs\via\VIA.exe' --type=renderer --field-trial-handle=1588,13949046230613957204,7885526779198114 13,131072 --disable-features=SpareRendererForSitePerProcess --lang=en-US --app-path='C:\Users\user\AppData\Local\Programs\via\resources\app.asar' --node-integration --no-sandbox --no-zygote --background-color=#fff --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=160771767 14480753997 --renderer-client-id=5 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1968 /prefetch:1 MD5: 0474F56BEB38D2AF8C20BB44D66CEBCA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

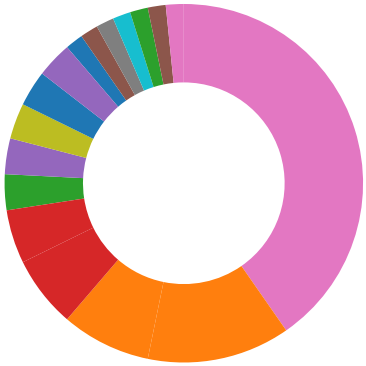
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	JoeSecurity_Predator	Yara detected Predator	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Yara detected Predator

Compliance:

Uses 32bit PE files

Creates a software uninstall entry

Creates license or readme file

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

E-Banking Fraud:

Yara detected Predator

Stealing of Sensitive Information:

Yara detected Predator

Remote Access Functionality:

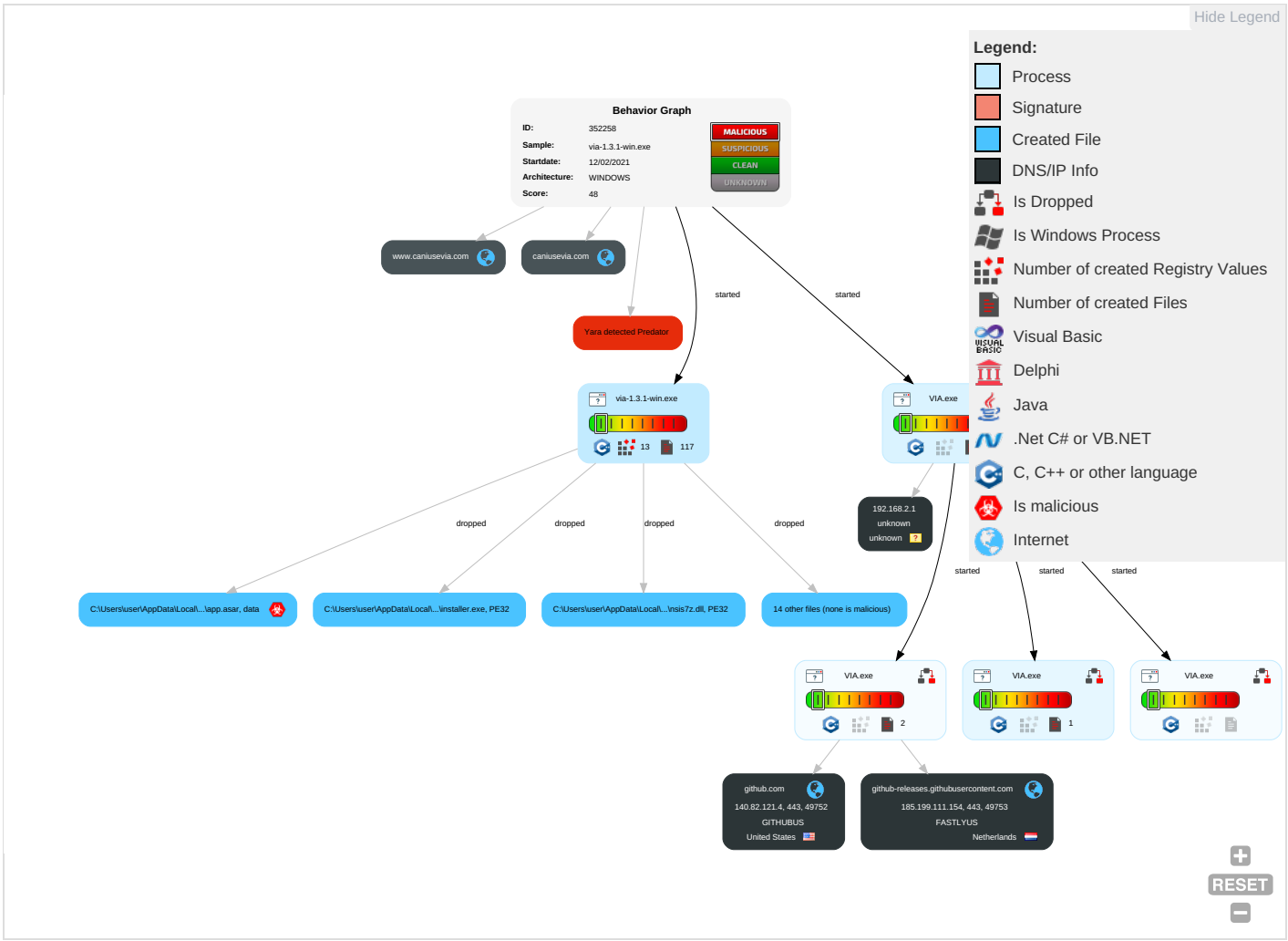
Yara detected Predator

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Command and Scripting Interpreter 1	Windows Service 1	Access Token Manipulation 1	Masquerading 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdr Insecure Network Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Default Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Windows Service 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 2	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Application Layer Protocol 2	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access

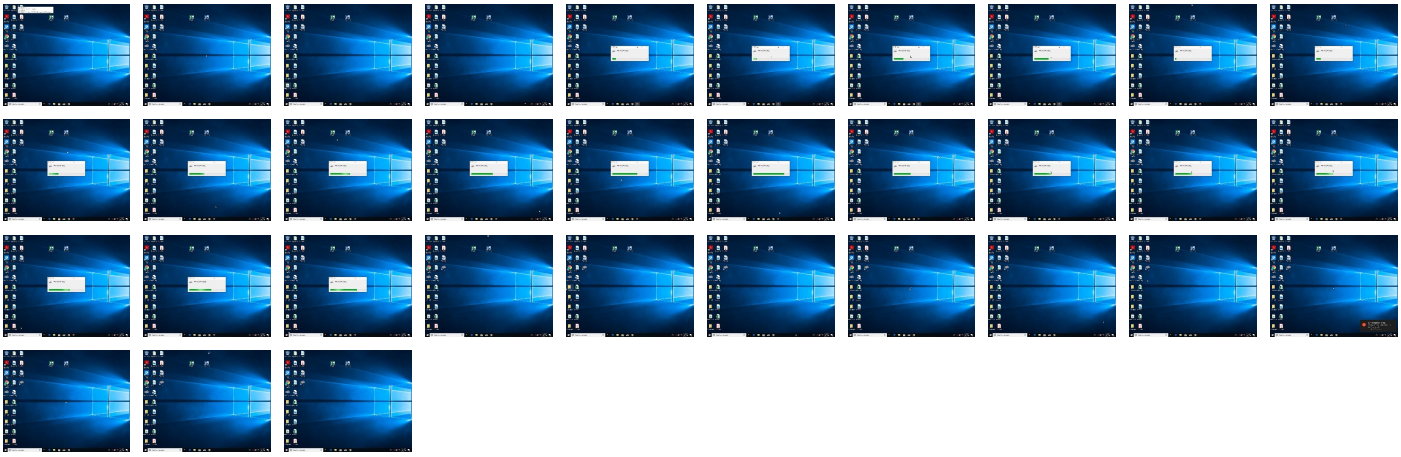
Behavior Graph



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
via-1.3.1-win.exe	0%	Virustotal		Browse
via-1.3.1-win.exe	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe	6%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\VIA.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\ffmpeg.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\libEGL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\swiftshader\libEGL.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Programs\via\swiftshader\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\SpiderBanner.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\SpiderBanner.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.caniusevia.com	0%	Virustotal		Browse
caniusevia.com	0%	Virustotal		Browse
github-releases.githubusercontent.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.startssl.com/policy.pdf04	0%	URL Reputation	safe	
http://www.startssl.com/policy.pdf04	0%	URL Reputation	safe	
http://www.startssl.com/policy.pdf04	0%	URL Reputation	safe	
http://www.startssl.com/policy.pdf04	0%	URL Reputation	safe	
http://https://dns11.quad9.net/dns-query	0%	Virustotal		Browse
http://https://dns11.quad9.net/dns-query	0%	Avira URL Cloud	safe	
http://unisolated.invalid	0%	Avira URL Cloud	safe	
http://report-example.test/testP	0%	Avira URL Cloud	safe	
http://https://tc39.github.io/ecma262/#sec-%iteratorprototype%-object	0%	Avira URL Cloud	safe	
http://chrome-devtools-frontend.appspot.com/serve_rev/%s/%s.html	0%	Avira URL Cloud	safe	
http://chrome-devtools-frontend.appspot.com/serve_rev/%s/%s.html/devtools/page/%s?ws=%s%s%sMalformed	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://www.startssl.com/policy0	0%	URL Reputation	safe	
http://www.startssl.com/policy0	0%	URL Reputation	safe	
http://www.startssl.com/policy0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://report-example.test/test	0%	Avira URL Cloud	safe	
http://crbug.com/490015	0%	Avira URL Cloud	safe	
http://www.startssl.com/sfsca.crl0	0%	URL Reputation	safe	
http://www.startssl.com/sfsca.crl0	0%	URL Reputation	safe	
http://www.startssl.com/sfsca.crl0	0%	URL Reputation	safe	
http://aia.startssl.com/certs/ca.crt02	0%	URL Reputation	safe	
http://aia.startssl.com/certs/ca.crt02	0%	URL Reputation	safe	
http://aia.startssl.com/certs/ca.crt02	0%	URL Reputation	safe	
http://html4/loose.dtd	0%	Avira URL Cloud	safe	
http://https://log.getdropbox.com/hpkp0	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/encrypted-media/#direct-individualization.	0%	Avira URL Cloud	safe	
http://https://dns.google/dns-query	0%	Avira URL Cloud	safe	
http://.css	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0;	0%	Avira URL Cloud	safe	
http://https://heycam.github.io/webidl/#dfn-default-iterator-object	0%	Avira URL Cloud	safe	
http://https://heycam.github.io/webidl/#es-iterable-entries	0%	Avira URL Cloud	safe	
http://https://wicg.github.io/cors-rfc1918/	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://https://chrome-devtools-frontend.appspot.com/	0%	Avira URL Cloud	safe	
http://https://tc39.github.io/ecma262/#sec-object.prototype.tostring	0%	Avira URL Cloud	safe	
http://https://crbug.com/v8/8520	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
github.com	140.82.121.4	true	false		high
www.caniusevia.com	18.198.68.141	true	false	• 0%, Virustotal, Browse	unknown
caniusevia.com	167.99.137.12	true	false	• 0%, Virustotal, Browse	unknown
github-releases.githubusercontent.com	185.199.111.154	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://url.spec.whatwg.org/#concept-url-origin	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-NonemptyClassRangesNoDash	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://invisible-island.net/ncurses/terminfo.ti.html#toc-_Specials	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#sec-atomescape	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://www.startssl.com/policy.pdf04	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doh.familyshield.opendns.com/dns-query	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://ocsp.starfieldtech.com/08	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-Atom	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://gist.github.com/XVilka/8346728#gistcomment-2823421	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://github.com/nodejs/node-v0.x-archive/issues/2876.	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://ocsp.starfieldtech.com/0;	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://console.spec.whatwg.org/#table	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://crashpad.chromium.org/https://crashpad.chromium.org/bug/new	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://console.spec.whatwg.org/#console-namespace	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://repository.certum.pl/ca.cer09	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high

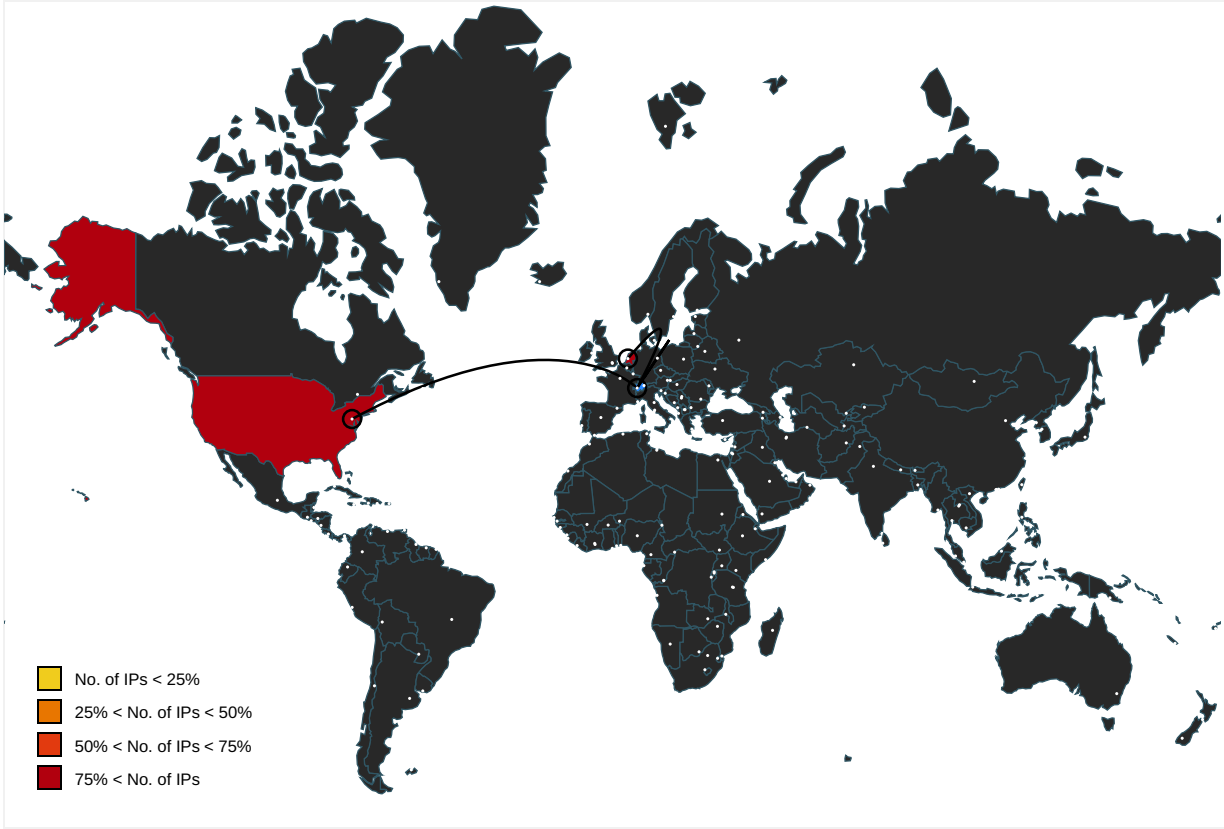
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns11.quad9.net/dns-query	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/nodejs/node/issues/13435	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-ClassAtomNoDash	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://goo.gl/t5IS6M).	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://tools.ietf.org/html/rfc7230#section-3.2.2	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://unisolated.invalid	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://report-example.test/testP	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/nodejs/node/commit/f7620fb96d339f704932f9bb9a0dceb9952df2d4	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-ClassAtom	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-annexB-Assertion	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://tc39.github.io/ecma262/#sec-%iteratorprototype%-object	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://url.spec.whatwg.org/#concept-urlencoded-serializer	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://www.certum.pl/CPS0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://nodejs.org/api/fs.html	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://github.com/chalk/ansi-regex/blob/master/index.js	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://github.com/nodejs/node/pull/21313	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://l.twimg.com/i/hpkp_report	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-ClassRanges	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://crashpad.chromium.org/	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://github.com/electron/electron/pull/17464	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-NonemptyClassRanges	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://www.midnight-commander.org/browser/lib/tty/key.c	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://nodejs.org/	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://tools.ietf.org/html/rfc7540#section-8.1.2.5	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-ControlEscape	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://certs.godaddy.com/repository/1301	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.alphassl.com/repository/03	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-Hex4Digits	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://www.squid-cache.org/Doc/config/half_closed_clients/	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-DecimalEscape	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-annexB-ClassControlLetter	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://chrome-devtools-frontend.appspot.com/serve_rev/%s/%s.html	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doh.opendns.com/dns-query	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://chrome-devtools-frontend.appspot.com/serve_rev/%s/%s.html/devtools/page/%s?ws=%s%s%sMalformed	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.rootca1.amazontrust.com0:	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.startssl.com/policy0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://certs.godaddy.com/repository/0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://certificates.godaddy.com/repository/gd_intermediate.crt0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://www.symauth.com/cps0(	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://www.thawte.com/cps0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-CharacterClassEscape	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://crl.godaddy.com/gdroot-g2.crl0F	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://crl.rootg2.amazontrust.com/rootg2.crl0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://csp.yahoo.com/beacon/csp?src=yahoocom-hpkp-report-only#	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://report-example.test/test	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa0)	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://crbug.com/490015	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.startssl.com/sfsca.crl0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.symauth.com/rpa00	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://goo.gl/yabPexextra_keys_may_be_added_here.	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://aia.startssl.com/certs/ca.crt02	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.ecma-international.org/ecma-262/#sec-line-terminators	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/2048ca.crl0;	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://www.chromestatus.com/feature/5527160148197376	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-Pattern	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://html4/loose.dtd	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	low
http://https://log.getdropbox.com/hpkp0	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://w3c.github.io/encrypted-media/#direct-individualization.	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://certs.starfieldtech.com/repository/0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://github.com/nodejs/node/pull/12342	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://crashpad.chromium.org/bug/new	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://github.com/Microsoft/TypeScript/issues/1863	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://aia1.wosign.com/ca1-class3-server.cer0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://dns.google/dns-query	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ecma-international.org/ecma-262/8.0/#prod-annexB-ExtendedAtom	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://.css	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	low
http://ocsp.thawte.com0;	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	low
http://https://heycam.github.io/webidl/#dfn-default-iterator-object	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://heycam.github.io/webidl/#es-iterable-entries	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wicg.github.io/cors-rfc1918/	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://invisible-island.net/xterm/ctlseqs/ctlseqs.html	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://subca.ocsp-certum.com0.	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://html.spec.whatwg.org/multipage/browsers.html#concept-origin-opaque	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.chromestatus.com/feature/5644273861001216.NavigatorVibrate	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://github.com/da-x/rxvt-unicode/tree/v9.22-with-24bit-color	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://github.com/nodejs/node/issues	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://https://www.ecma-international.org/ecma-262/8.0/#prod-HexDigits	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false		high
http://www.wosign.com/policy/0	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://chrome-devtools-frontend.appspot.com/	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/g2ca.crl0;	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false		high
http://https://www.chromestatus.com/feature/5742188281462784.CancelDeferredNavigationWillRedirectRequestWil	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false		high
http://https://tc39.github.io/ecma262/#sec-object.prototype.tostring	VIA.exe, 00000011.00000000.427499385.00007FF7ECDC9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/v8/8520	VIA.exe, 00000011.00000000.422760140.00007FF7EC3C9000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	VIA.exe, 00000011.00000000.429516213.00007FF7ED2E8000.00000002.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
140.82.121.4	unknown	United States		36459	GITHUBUS	false
185.199.111.154	unknown	Netherlands		54113	FASTLYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	352258

Start date:	12.02.2021
Start time:	05:32:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	via-1.3.1-win.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.troj.winEXE@7/95@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 95.6% (good quality ratio 94.2%) • Quality average: 86.1% • Quality standard deviation: 21.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 40.88.32.150, 168.61.161.212, 51.11.168.160, 23.218.208.56, 93.184.221.240, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.104.144.132, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory 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.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
140.82.121.4	SecuriteInfo.com.Trojan.PackedNET.535.22246.exe	Get hash	malicious	Browse	
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	
	82e6033fb85f4abe59e16cb29c9faca2.exe	Get hash	malicious	Browse	
	5aa085f0fa8592460e391052db9c94cd.exe	Get hash	malicious	Browse	
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	
	1464bbe24dac1f403f15b3c3860f37ca.exe	Get hash	malicious	Browse	
	Require_Quote_20200128 SSG.pdf ind.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	purchase order TR2021011802.exe	Get hash	malicious	Browse	
	33f77d4d.exe	Get hash	malicious	Browse	
	RFQ_211844_PR20Q-6706.pdf.exe	Get hash	malicious	Browse	
	P.O.No.#17AUFR010S.pdf.exe	Get hash	malicious	Browse	
	PO#83922009122.pdf.exe	Get hash	malicious	Browse	
	AS006-20211201.pdf.exe	Get hash	malicious	Browse	
	2CBPOfVTs5QeG8Z.exe	Get hash	malicious	Browse	
	Payment.exe	Get hash	malicious	Browse	
	HashUpUtility.sfx.exe	Get hash	malicious	Browse	
	DHL_document1102202068090811.exe	Get hash	malicious	Browse	
	soa1.exe	Get hash	malicious	Browse	
185.199.111.154	http://https://www.canva.com/design/DAEKC1MKSQM/ESg5NnPu3it211SCpnfI7A/view?utm_content=DAEKC1MKSQM&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	
	http://https://www.w3.org/1999/xhtml	Get hash	malicious	Browse	
	http://directline.botframework.com	Get hash	malicious	Browse	
	http://tinyurl.com/impeachackerman	Get hash	malicious	Browse	
	http://cloud.wpakademi.com	Get hash	malicious	Browse	
	http://ncehk20l9.github.io	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
github.com	Farie PO.doc	Get hash	malicious	Browse	• 140.82.121.3
	SecuriteInfo.com.Trojan.PackedNET.535.22246.exe	Get hash	malicious	Browse	• 140.82.121.4
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	• 140.82.121.3
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 140.82.121.4
	82e6033fb85f4abe59e16cb29c9faca2.exe	Get hash	malicious	Browse	• 140.82.121.4
	5aa085f0fa8592460e391052db9c94cd.exe	Get hash	malicious	Browse	• 140.82.121.4
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 140.82.121.4
	cbf708XSsON55d9B49dt.exe	Get hash	malicious	Browse	• 140.82.121.3
	d0b443110cf5a7bd05759c00fee8fdad.exe	Get hash	malicious	Browse	• 140.82.121.3
	1464bbe24dac1f403f15b3c3860f37ca.exe	Get hash	malicious	Browse	• 140.82.121.4
	84ab43f7eda35ae038b199d3a3586b77.exe	Get hash	malicious	Browse	• 140.82.121.3
	ORDEN.exe	Get hash	malicious	Browse	• 140.82.121.3
	Require_Quote_20200128 SSG.pdf ind.exe	Get hash	malicious	Browse	• 140.82.121.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation.exe	Get hash	malicious	Browse	• 140.82.121.3
	client.exe	Get hash	malicious	Browse	• 140.82.121.3
	purchase order TR2021011802.exe	Get hash	malicious	Browse	• 140.82.121.4
	TNT Original Invoice PDF.exe	Get hash	malicious	Browse	• 140.82.121.3
	Photo-064-2021.jpg.exe	Get hash	malicious	Browse	• 140.82.121.3
	33f77d4d.exe	Get hash	malicious	Browse	• 140.82.121.4
	RFQ_211844_PR20Q-6706.pdf.exe	Get hash	malicious	Browse	• 140.82.121.3

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	2200.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon48_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 151.101.1.195
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	• 151.101.1.44
	#U2261#U0192#U00f4#U20a7.htm.htm	Get hash	malicious	Browse	• 151.101.65.195
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	• 151.101.1.44
	8.prtyok.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Bulz.349310.9384.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Razy.840176.14264.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Bulz.349310.24122.dll	Get hash	malicious	Browse	• 151.101.1.44
	login.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	pfjgWtj6ms.exe	Get hash	malicious	Browse	• 151.101.64.119
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• 151.101.1.211
	footer.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	SCAN_PO210205.exe.exe	Get hash	malicious	Browse	• 185.199.111.153
	Farie PO.doc	Get hash	malicious	Browse	• 151.101.13.188
	acr1.dll	Get hash	malicious	Browse	• 151.101.1.44
	TRIGANOcr.dll	Get hash	malicious	Browse	• 151.101.1.44
	ct.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.PackedNET.535.22246.exe	Get hash	malicious	Browse	• 151.101.0.133
GITHUBUS	Farie PO.doc	Get hash	malicious	Browse	• 140.82.121.3
	SecuriteInfo.com.Trojan.PackedNET.535.22246.exe	Get hash	malicious	Browse	• 140.82.121.4
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	• 140.82.121.4
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 140.82.121.4
	82e6033fb85f4abe59e16cb29c9faca2.exe	Get hash	malicious	Browse	• 140.82.121.4
	5aa085f0fa8592460e391052db9c94cd.exe	Get hash	malicious	Browse	• 140.82.121.4
	ace80239facd926583cb2f9ceb84bb9c.exe	Get hash	malicious	Browse	• 140.82.121.4
	cbf708XSsON55d9B49dt.exe	Get hash	malicious	Browse	• 140.82.121.3
	d0b443110cf5a7bd05759c00fee8fdad.exe	Get hash	malicious	Browse	• 140.82.121.3
	1464bbe24dac1f403f15b3c3860f37ca.exe	Get hash	malicious	Browse	• 140.82.121.4
	84ab43f7eda35ae038b199d3a3586b77.exe	Get hash	malicious	Browse	• 140.82.121.3
	ORDEN.exe	Get hash	malicious	Browse	• 140.82.121.3
	Require_Quote_20200128 SSG.pdf ind.exe	Get hash	malicious	Browse	• 140.82.121.4
	Quotation.exe	Get hash	malicious	Browse	• 140.82.121.4
	client.exe	Get hash	malicious	Browse	• 140.82.121.3
	purchase order TR2021011802.exe	Get hash	malicious	Browse	• 140.82.121.4
	TNT Original Invoice PDF.exe	Get hash	malicious	Browse	• 140.82.121.3
	33f77d4d.exe	Get hash	malicious	Browse	• 140.82.121.4
	RFQ_211844_PR20Q-6706.pdf.exe	Get hash	malicious	Browse	• 140.82.121.4
	P.O.No.#17AUFR010S.pdf.exe	Get hash	malicious	Browse	• 140.82.121.4

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	eTrader-0.1.0.exe	Get hash	malicious	Browse	
	eTrader-0.1.0.exe	Get hash	malicious	Browse	
	w0Ku4mr4HN.exe	Get hash	malicious	Browse	
	w0Ku4mr4HN.exe	Get hash	malicious	Browse	
	http://https://rpmi.aspire.co/ucs/dl/micollab_pc.msi	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	elior-1.13.4.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	eTrader-0.1.0.exe	Get hash	malicious	Browse	
	eTrader-0.1.0.exe	Get hash	malicious	Browse	
	SlackSetup.exe	Get hash	malicious	Browse	
	RefinitivWorkspace-installer_1.11.385.exe	Get hash	malicious	Browse	
	http://https://timeular-desktop-packages.s3.amazonaws.com/win/production/Timeular_Setup.exe	Get hash	malicious	Browse	
	SlackSetup.exe	Get hash	malicious	Browse	
	SlackSetup.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Programs\via\LICENSE.electron.txt	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	5.127745905239685
Encrypted:	false
SSDEEP:	24:lDiJHxRHuyPP3GtIHw1Gg9QH+sUW8Ok4F+d1o36qjFD:lDiJzfPvGt7ICQH+sfIte36AFD
MD5:	F8436F54558748146EC7EBD61CA6AC38
SHA1:	EF226E5B023D458EFCDC59DC653694D89802F81C
SHA-256:	34F6F27C26D1BB8682EBB42AE401F558228FD608455BD7C6561D5FD500B7D05B
SHA-512:	5B310B48BBEE286F03E645E4BFAD0EC870A7C68C445D54F46F3EAAA9C427F9DE6CD0561D451838BD53C78A5289E9F0BDA19CDA4257A4657580AFA6C35791300
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Copyright (c) 2013-2019 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 no tice 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 C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION.WITH

C:\Users\user\AppData\Local\Programs\via\LICENSES.chromium.html	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4723060
Entropy (8bit):	4.895382261104505
Encrypted:	false
SSDEEP:	24576:3sOBLmnLiLxsmrwrDK7qcj/kUg7wWnQJ8um:cGLmLAKUuObjhJ6
MD5:	C91C1D7D87F2EC9AEC7EFA9D34808000
SHA1:	5325EEB991FB27FCB8640AC3B272AB387A884EB4
SHA-256:	67885E1586ECF0354E79467340CEBE4D977B8DDCB432F7E832008B4FF3C8A1FF
SHA-512:	6DC0E6518CC682E26572FCC4627AD2A5A616931B4F9FC328A12272876E9139CEEFA8BB8164984DE6F574E8D76952CF206C79F1AF6C9E75EAFD92A37619A9D73
Malicious:	false
Reputation:	low
Preview:	Generated by licenses.py; do not edit. --><!doctype html>..<html>..<head>..<meta charset="utf-8">..<meta name="viewport" content="width=device-width">..<titl e>Credits</title>..<link rel="stylesheet" href="chrome://resources/css/text_defaults.css">..<style>..body {.. background-color: white;.. font-size: 84%;.. max-width: 1 020px;..}...page-title {.. font-size: 164%;.. font-weight: bold;..}...product {.. background-color: #c3d9ff;.. border-radius: 5px;.. margin-top: 16px;.. overflow: auto;.. pa dding: 2px;..}...product .title {.. float: left;.. font-size: 110%;.. font-weight: bold;.. margin: 3px;..}...product .homepage {.. color: blue;.. float: right;.. margin: 3px;.. text- align: right;..}...product .homepage::before {.. content: " - ";..}...product .show {.. color: blue;.. float: right;.. margin: 3px;.. text-align: right;.. text-decoration: underline;.. }...licence {.. background-color: #e8eef7;.. border-radius: 3px;.. clear: both;.. display: none;.. padd

C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	484880
Entropy (8bit):	4.129934504383048
Encrypted:	false

C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe	
SSDEEP:	3072:Wa77v0JhE4Dy6LtauRGVp35+u7Mv0P5Qw2tvhOEA1RJCir86SrSrvZwa3j:Ww4JQ6xBGVp35+uwv0Pj2t0EyL+ewaT
MD5:	F8FFB3040F9691B9C119E39A093BF55D
SHA1:	9C926BFCD8EF6CD65C9276D760AED3A0F688554A
SHA-256:	F2FFC39FF8CFB4AEBAE59B841FB973E399202B8BA4DD83B3F29D6E129EF7247A
SHA-512:	A69D02E6EE8DC0292047836DA49D56720D4F54C295205ED51F1C2F2C0C106EBDBA0C0CFBA5E901C499D8C3549A4FFF4F301CC50B07BB9B15B09D7E2EF80603 7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Reputation:	low
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...|.oZ.....h...8...@...3.....@.....@.....0..... .....text...'f.....h..... ..`.rdata.....I.....@..@.data.....@....ndata.....rsrc.....0.....@..@..... ....

C:\Users\user\AppData\Local\Programs\via\VIA.exe	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	104941568
Entropy (8bit):	6.659514714368976
Encrypted:	false
SSDEEP:	786432:NnqJaAlcRQpFYgegURVwiHS+MWD3/e/88a/DReHRQqGLdRR/bHzPQTWco:wJaAlSQpFTjEVhHEQ/e/fGNYQHLHRjk
MD5:	0474F56BEB38D2AF8C20BB44D66CEBCA
SHA1:	BBD0F66A20B84A70759A83D9ED43C9BE835799DE
SHA-256:	DAD702C72F76C8D517D670624E942C29AA85FE583F936D3ABE7E7857E8DCEAED
SHA-512:	792CA78BA5F0D91F78971B3FA3B7B28C2D26848BAAC9B923DF6D82A7DC057C587E54C748848244182D22C74E05BE941AFCFA66ABCD1D78700D59F762A19D79(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...,..].FA.....".....v....^.....@.....M.....`..... .....;.dw.....t4-.....@B.HK.....(...@.....!.....text....t.....v..... ..`.rdata...i.....j...z..... @..@.data.....@....pdata..t4-.....6-.....@..@.00cfg.....P;.....6/.....@..@.retplne`....`;.....8/.....rodata.`....p;.....:/.....@..@.tls.....;. .....R/.....@...CPADinfo8....;.....T/.....@...prot.....;.....V/.....@..@.rsrc...dw...;..x...X/.....@..@.reloc..HK...@B..L....5.....@..B/4.....:+....M.,....A... .....@..B.....

C:\Users\user\AppData\Local\Programs\via\chrome_100_percent.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	177830
Entropy (8bit):	7.835273501069481
Encrypted:	false
SSDEEP:	3072:xHsSzwVnp5NiU2w5+vfdYCJdx1+khejSTS9SO0vVm7O0U27IIABNHlJngfI:xHsSzwVXMUx5c1YC7x1+fSucY7OP2ITL
MD5:	C56BC01C88F2FD186AE22F10B1BD5900
SHA1:	B000E68CCD919010EFF8C2E114B7D1B6E702D997
SHA-256:	D8CBC2234F40B49437A5876BB008B6B43AFDF92391DEC3F0739BE98E448AB671
SHA-512:	46F9158E0F06A4E415B95A7DABE88CC4F3EECC235CDAF9D744CAF4DE5E665AE91599E3C2FEEA0860E9F6EEB2EEA45FE4E57542FAE95ED9110D44624513DE3 AA0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....C.....C.....C.....C.....C7....C.....C.....C.....D.....D.....D5....D.....D. ...DA!...D."...D.#...D.,..8c./..9c<0..:c.1..;c.4..<c.7...d.;...d.<...dJ>...d.?...d.@...d4A..dd.A..edJ...fd ....xi|...yi....zi....{i....|i...}i....~i.....i5....i.....i.....i.....i.....i.....i/....i.....i.....i.....ib....i.....i1....i ....i.....i.....i;....i$....iJ....i.....i'....i.....i.....i%....i.....iC....i.....iT....i.....iX....i.....i.)...i[*...im,...i.....iC/. ..i%0...i.0...i.1...i.1...i.2...i.2...i.3...i.4...in5...ia6...i.7...i9:...i.<...i.A...ioF...iDG...i.H...i.I...i.J...imK...iMM...i+O...i.Q...i.....i.....iX....i.....i.....i+~...i.~...i.....i3....i*....i.....in....i.....iT....i. ...i|....iF....i.....i.....i.....iC....i.....i.....i.....iC....iz....ip....ig....iv....k^....k.....k.....kW....k.....k ....k....k7....k.....k....k%....km....k.....kk....k....kk....k....kx....k.....k.....k.....k.....ke....k.... k%....k.....kG....k.....k.....k^....k.....k.....k.....k....kB....k..

C:\Users\user\AppData\Local\Programs\via\chrome_200_percent.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	315644
Entropy (8bit):	7.922192633378286
Encrypted:	false
SSDEEP:	6144:SDQYaReMYz73QYV85u/oFwvwoytKi6obByPGlPFYKxo+:3fIJg5u/oFdpxLlFYK
MD5:	9662C1F572EF83F070D2354B0275EC60

C:\Users\user\AppData\Local\Programs\via\chrome_200_percent.pak	
SHA1:	04CE905A95A1C3B8521A17AC9F57503E7AA3EAC9
SHA-256:	55DD419A1CECCA86665BA5E6184D6B58EDF714D652E67C5220DD3B407D99AFA8
SHA-512:	B1D34D58F5079B1DB9764BCE2787969113AC7CB1B83DBC3EBCE8C9C287AF372A639611BA11246A088243E2098DBD1D6AD51341EFF2A57A995868BB0DB94A31 7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....C.....C.....C.....C.....C.....C.....C.#...C.(...D.+...D^3...D.7...D.9...D.;...D.=...DU@...D.@...DxU..8c.Z..9c.^..:c.a..;c.d..<c.g...d.k...d.l...d4n...d.o...d|p...d.q..dd.q ..ed4...fd....xif...yi....ziK...{iT...|i....}i....~iM....i.....i.....i{....i.....i.....i.....iG....i2....i^....iR....i.....i.....i.....i.'...i[0...i.2...iN5...io9...i.@...i.A...i.F...i.I...i.M...i.S...i.T...i.W...i.Z...i.]...i.a...i.h...i.l ...iB....i9....i ....i.....i6....iP....iT....i.....i.....i.....i8....i.....i+....i.....i{....i.....i.....i.....i.....is....i.....i/....i.....i.....iI....i.....io....i\....i$....i.....i.....i@....i_H...i.I...i.J...iML...i.....ikv...i.w...iUy...i.{...iP| ...ik....i.....i.....iz....iB....i8....i[....i.....i.....i.....i.....i.....i.....i.....i.....i.....ir....i.....i.....k.....kN....k.....k.....k.....k.....k#....k.....k....k5....k.....k.....k.....k*....k.....kE....k.....ks....k.....k.....k@.. ..k.....kQ....k.....k_....k#....k.....k9....k.....k.....k.....kj....k..

C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4481992
Entropy (8bit):	6.374831048870993
Encrypted:	false
SSDEEP:	49152:cwBNwAqRvTvbehyCZ5xRmhErU6jFyU+dQZTHchy0eQago4I+oiP85+hA6+Se4QQU:SUZ5P7FwcAgLbz+3s0Bm
MD5:	FEA40E5B591127AE3B065389D058A445
SHA1:	621FA52FB488271C25C10C646D67E7CE5F42D4F8
SHA-256:	4B074A3976399DC735484F5D43D04B519B7BDEE8AC719D9AB8ED6BD4E6BE0345
SHA-512:	D2412B701D89E2762C72DD99A48283D601DD4311E3731D690CC2AB6CCED20994FA67BF3FEA4920291FC407CD946E20BDC85836E6786766A1B98A86FEBAA0E3 9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: eTrader-0.1.0.exe, Detection: malicious, Browse • Filename: eTrader-0.1.0.exe, Detection: malicious, Browse • Filename: SlackSetup.exe, Detection: malicious, Browse • Filename: RefinitivWorkspace-installer_1.11.385.exe, Detection: malicious, Browse • Filename: , Detection: malicious, Browse • Filename: SlackSetup.exe, Detection: malicious, Browse • Filename: SlackSetup.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.\.i.\.i.\K2.].i.\K2.].i.\...].i.\..0\.i.\.i.\ m.\...].i.\...].i.\...].i.\...]'i.\..^\.i .\..\\.i.\...].i.\Rich.i.\.....PE..d.....c....." .....V3..t.....d&.....E.....D...`A.....A.x.....A.....pD.@....`B.....BD..!....D. .....>.T.....8.6.(...0.6.....`.6.....text....U3.....V3..... ..`.rdata.....p3.....Z3.....@..@.data....#...0A.....A.....@....pdata.....`B.. .....A.....@..@.rsrc...@....pD.....C.....@..@.reloc.....D.....C.....@..B.....

C:\Users\user\AppData\Local\Programs\via\ffmpeg.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2128896
Entropy (8bit):	6.610063741379285
Encrypted:	false
SSDEEP:	49152:u+cOvGFd/RIgWtRZgE3A0bsPSZAjhwFo7zMYq/X+838tUy1zp:uDOvkOjtRZgEwykU4p
MD5:	3B4B100BA3AE61391DA61F5B355B1183
SHA1:	5BFA099074789D8337CD92E50ED00B100AC5B527
SHA-256:	1922C8DD5C693DE0084DAC00E346D40BDDB806C40151F0E8E29E5F67CE1FD0A2
SHA-512:	BA3D67241CE070737AF1BEFAD3C9710F1D567EB8DE29B8B9BACFFD28820779C4CF54EF57F209F0813AAF5110D7E330EC7EF29548CCE7A40E1B4AECED1B81B CD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...,..]....." .....N...*..... 3.....`..... .....U.....Z..(.....P2.....2.....@T.....`c.....]....text....L.....N..... ..`.rdata..`>...`...@...R.....@ ..@.data.....0.....@....pdata.....P2.....@..@.00cfg.....2.....J .....@..@.reloc.....2..0...L .....@..B.....

C:\Users\user\AppData\Local\Programs\via\icudtl.dat	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Programs\via\icudtl.dat	
Size (bytes):	10426784
Entropy (8bit):	6.218401047383452
Encrypted:	false
SSDEEP:	196608:wzwSv9AA0fJlt5liXUxR0rHc93WhlA6t9QJGX2EXmJNVR2m:9Kl0fJlliXUxR0rHc93WhlA6t9QJGX2z
MD5:	9E8B247AA7A609E6632518ECD6634FC0
SHA1:	CC43315BEC76167BE7DFBB7DD0B6D61974204D6C
SHA-256:	18ACC07D9CA59B1E599343B022A9E602A0A0C152866F7E5DCE1FEDD2DBCD33A0
SHA-512:	7A9590F410C14886317D7CDAE606B50B4A0355061E251AA3BCD3E0C614438298E839FF116553089116423E9BC98C131F35796478517D88A180A5A2D08FF7FA5F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	...'.....CmnD..... Copyright (C) 2016 and later: Unicode, Inc. and others. License & terms of use: http://www.unicode.org/copyright.html .....t).....)....)..`....)..`....)....)..`....)....)....)..p....*.....$*.....7*..0...J*.....]*.....p*.....*.....*.....*.. ....*.....*.....*.....*.....+.....+.. ....+..p...A+.....T+.. ...g+.....z+..0 ...+... ...+..."...+..p"...+..@$...+...$..+.. %...+..p%...,...%...,...&..+,...X..B,..0{..R,.....b,.. ....,.....,..0....,...v&..,....&..,.. .&..,....&..-..`.&..-....&.E-....&.\-..@.&.s-..p.&..-....(..-.. .(..-....)..-...{*.....@X+.)...p),.L.....-.c.....-.....-.....0.-.....-.....-.....1.../..`.0../..`m0.7/....1.N/.. .1.j/..0.1.z/....1../..`J1../...J1../...m1../...o1../....1../..`.1..0..p!2..0...E2./0...i2.D0..`.2.Y0..@(3.o0...(3..0...N3..0...N3..0...P3..0...P3..0.. Q3..0....3..1....3.61....3.K1..@.3.`1.. .3.u1....4..1...4..1..@.4..1....4..1.. .4..1.. .4..1..p.4..2....5.$2...c5.92..P.5.N2....5.f2...5.{2..

C:\Users\user\AppData\Local\Programs\via\libEGL.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	141824
Entropy (8bit):	6.165415939182816
Encrypted:	false
SSDEEP:	3072:Hu1goINM1Rn1Pd9rN+xrBXs0AZ8ia5od09XPgFSN/:HYB+iBD9R+780AZ+v79
MD5:	C2F9D30C9AC6C3D2443929CC849A0520
SHA1:	3FC8D7F936819773966ADC02B8F5DBD0533E5178
SHA-256:	88626E89D063C80AA5D73CED0671398A04F71723D2EC790DE911B74646126370
SHA-512:	AC9AF876E85BD26C07072DB5E1BF20D03CD3F8CFE519F787598FF4AFD881AB11377602555A5FFE99F6C375DCDAF3339D4AD919D034B8F3A77132912519D6FE0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...,..]....."....>.....8.....`.....C.....(..... ....@..@.....x.....@...(... Z.....`.....text...&<.....>..... ..`.rdata.....P.....B..... @..@.data... .....@....pdata..@....@.....@..@.00cfg.....`.....@..@.tls.....p.....@....rsrc... .....@..@.reloc..x.....".....@..B.....

C:\Users\user\AppData\Local\Programs\via\libGLESv2.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7731200
Entropy (8bit):	6.183424530463462
Encrypted:	false
SSDEEP:	49152:Z430yYnlr+/9j2JzYP5YMVBtYKXUu+MHk5ktmveyBiXh3VfE4wfepY/23LdId74M:Z4xqY7YM/xweVPKi+EyJj/RrqGUs
MD5:	4D005AA42EB04216D26E5FB32B4981F6
SHA1:	A4005EEC963E7935C371B7A3A4ED7573D471CC0D
SHA-256:	1563C7F4EE97BE9F37620027229A9DF2467F1AE4671B380A8E8261B93EA99AC5
SHA-512:	01347D1C4C62623D12B7B26B71DC2E2C0EF4961B11B3B5965FCD081A97C266FC2C6B3DA85246EA62D0A8676D1EE715913FA426BDC6D0F0C4DF01BFE04036AC F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...,..]....."....xL..|).....}l.....`.....j.....l.x....P..8....p.....`..<-..|.j.....X.j.(....i.....`.l....@.j.@.....text...vL.....xL..... ..`.rdata.... ...L... ..|L.....@..@.data.....n..`m.....Fm.....@....pdata.....p.....r.....@..@.00cfg.....0.....t.....@..@.tls.....@.....t.....@....rsrc...8....P.....t.....@..@.reloc..<-...`.....t.....@..B.....

C:\Users\user\AppData\Local\Programs\via\locales\am.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	122392
Entropy (8bit):	5.0590622621002765
Encrypted:	false
SSDEEP:	3072:ZtlbZYiKP7wm8M77Rt4rgEkA0SqNmCoZb/qoGnZJjhSt+WWRIFBCkepJMt1H+i6O:9bdbQlpx30jH8+d
MD5:	3ED0D4542982E7F4C7970808E9DF9474

C:\Users\user\AppData\Local\Programs\via\locales\am.pak

<table>
<tr><td>SHA1:</td><td>E216CEA6E8BC4CBDEA9E1159A17D18469AE6C227</td></tr>
<tr><td>SHA-256:</td><td>E0EF4BA4FB1D4570123AC1311E67DA9358CC028FBC0A5816B563D4BA0179F5EA</td></tr>
<tr><td>SHA-512:</td><td>A4169242C8D6E9E51B02EA20F84A3C133796564517A77AE283FB2183343401B6471D5AEC81BB6347676F989F0283C7C881CECDCA1C55CF6DEC1F36480E0E412E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..+..~..+.....+.....+....&+....,+....;+....L+....U+....j+....w+....}+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....A,....`,.....,.....,.....,.....,.....,.....,....
.,.....,.....,.....,.....,.....,.....-....6-....I-....U-..!.e-..".h-...:.-...:.-...:.-...:.....;Y....;.....;.....;.....;.....;//...;M/...;t/...;./...;.0...;m0...;.0...;.0...;.1...;.1.. ;=1..#;L1..$;U1..%;l1..&;.1..(;.2..);12..*;J2
..+;i2..,;{2..-;.2...;.2../;.3..0;o4..3;>5..4;X5..5;.5..6;.5..7;.5..8;.6..9;.7..:;.7..;;Q8..<;.8..=;.8..>;.9..@;d:..A;.;..C;.;..D;.;..E;.;..F;.;..G;.<..H;;<..I;R<..J;{<..L;.<..M;.=..N;.>..O;.>..P;.>..
Q;.>..R;.A..S;;B..T;.C..U;.C..W;.C..Y;.C..Z;.C..[;.D..\;.D..];fD..b;.D..c;2E..d;.E..e;.F..f;1F..g;~F..h;.F..i;SG..j;.G..m;.H..p;\H..r;kH..s;qH..t;zH..u;.H..v;.H..w;.I..x;.I..y;.I..z;.I..{;NI
..|;kI..};.I..~;.I...;.I...;.I...;.I...;.J...;.J...;.K...;EK...;uK...;.K...;.K...;.K...;.K...;.K...;.K...;.K...;.K...;.K...;.K...;.K...;.K...;.L...;.L...;.L</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\via\locales\ar.pak

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>123569</td></tr>
<tr><td>Entropy (8bit):</td><td>5.140723968913605</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:aj4yHLNgjZhDWNYoQUWuMQwxHSM2uZtE9TYJFAj6ReyF5D0X2x91Y:aj4CNg3oU/DE</td></tr>
<tr><td>MD5:</td><td>A67BFD45825968D86CDCF91CD89310DF</td></tr>
<tr><td>SHA1:</td><td>B8455DEE614367BE4FA4D7669E650714024F607A</td></tr>
<tr><td>SHA-256:</td><td>1E894A2B00F957A913E1BA768FFCF30C29B570D2EAB307790FC761FA55F44225</td></tr>
<tr><td>SHA-512:</td><td>03FDA321FF4E342F58B02995929C382DEA8ECF2320C65900FE4996DEA1335235163092EB9BAD84CA6F33B086B3323A4D75991829730941CA3ECAA022BA14B160</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..*..~..+.....+.....+....$+....*+....9+....J+....S+....h+....u+....{+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....K,....d,.....,.....,.....,.....,.....,.....,.....,....
.,.....,.....-.....-....<-....^-....o-....y-..!..-..".-...:.-...:.-...:.-...:.....;P....;.....;.....;.....;.....;A/...;s/...;./...;./...;B0...;.0...;.0...;.1...;%1...;-1.. ;S1..#;Y1..$;e1..%;.1..&;.1..(;.2..);D2..*;^2..
+;y2..,;}2..-;.2...;.2../;.3..0;&4..1;.5..2;.5..3;.6..4;.6..5;.6..6;.6..7;+7..8;.7..:;.8..;;&9..<;i9..=;.9..>;.:..@;.;..A;_<..C;*=..D;9=..E;J=..F;]=..G;y=..H;.=..I;.=..J;.=..L;.>..M;.>..N;+@
..O;X@..P;}@..Q;.@..R;.D..S;.F..T;@H..U;.H..W;.H..Y;.H..Z;.I..[; I..\;9I..];.I..b;?J..c;.J..d;.K..e;JK..f;hK..g;.K..h;oL..i;.L..j;\M..m;.M..p;.M..q;.N..r;.N..s;.N..t;.N..u;KN..v;nN
..w;.N..x;.N..y;.N..z;.N..{;KO..|;jO..};.O..~;.O...;.O...;.O...;.P...;.P...;.Q...;NQ...;.Q...;.Q...;.Q...;.Q...;.Q...;.Q...;.Q...;.R...;.R...;.R...;.R...;!R...;%R...;3R...;6R...;DR</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\via\locales\bg.pak

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>133078</td></tr>
<tr><td>Entropy (8bit):</td><td>4.874700521695386</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:rEHWJsWXnzhqaWzMn6v63BMW3f4ZHrz3kZN0kN96aaGQAWosUV6DreF:w2Js8Dx6vjZHrzkZN0kN96lAWosUV6D6</td></tr>
<tr><td>MD5:</td><td>0B3155230E1942D238341C2F9EB88EF9</td></tr>
<tr><td>SHA1:</td><td>82590D918C0B2350DC46B2925D5550EE427B27E3</td></tr>
<tr><td>SHA-256:</td><td>0BEDA1647B0760046A7B18E4498A62B727B6320141E0A3B0CD864CABB7EB21ED</td></tr>
<tr><td>SHA-512:</td><td>FABFF8C3B1BC5B94AE8A27BE1D790FFEA85D7DE773AD48F2A2ECCCCC63EA35445F639349B5E5A59EC85E5378E7F0D1ADBBDEBDAC7C1F71F71FC5E64CE9D
0AD4E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..+..}..+..~.*+....2+....7+....D+....J+....Y+....j+....s+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.... ,....9,....V,.....,.....,.....,.....,.....-.....-.....-.... -
....!-....2-....U-...._-....s-.....-.....-.....-.....-..!..-..".-...:.....:7....:.....:.....;*/...;./...;./...;.0...;-0...;.0...;.0...;.1...;)1...;.1...;|2...;.2...;.2...;.3...;.3.. ;E3..#;W3..$;c3..%;.3..&;.3..(;34..);z4..*;.4
..+;.4..,;.4..-;.5...;x5../;T6..0;.7..1;.7..2;.8..3;.9..4;.9..5;.9..6;.:..7;P:..8;;;..9;p<..:;.<..;;B=..<;.=..>;.>..A;.>..C;.?..D;.?..F;.?..G;.?..H;.@..I;/@..J;V@..L;.@..M;.A..N;PB..O;]B..P;
tB..Q;.B..R;oD..S; E..T;.E..U;VF..W;.F..Y;.F..Z;.F..[;.F..\;.F..];MG..b;.G..c;BH..d;.I..e;7I..f;ZI..g;.I..h;rJ..i;.K..j;.K..m;.K..p;JL..r;dL..s;nL..t;zL..u;.L..v;.L..w;.M..x;.M..y;7M..z;:M..
{;.M..|;.M..};CN..~;PN...;fN...;uN...;.N...;lO...;.O...;5P...;.P...;.P...;.P...;.P...;.P...;.P...;.P...;.P...;.P...;.Q...;.Q...;.Q...;.Q...; Q...;"Q...;(Q...;2Q</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\via\locales\bn.pak

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>173570</td></tr>
<tr><td>Entropy (8bit):</td><td>4.471779065996595</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:K/mX1cWripiuRr18JMgylH0mvRZrWChokW:WmlcWri3dm</td></tr>
<tr><td>MD5:</td><td>238816F58B8247ED3D95538C5B4CE5D8</td></tr>
<tr><td>SHA1:</td><td>5AC704AEE7070779B1DEED3C6578DC8962076432</td></tr>
<tr><td>SHA-256:</td><td>62952441557CA8893B925196DC3C4CC89989237A1579786217E429845818A010</td></tr>
<tr><td>SHA-512:</td><td>A3A486924032850AA73456E83147E831C5DA15BBFADCD669C917F01FBE7DD90A2FCB9EFD9BFFA6B7411D0D0C7DA331D5E990FA3D3C098F5FBFBCDA75B06D9
7C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\via\locales\bn.pak

Preview:


```
...........|..*..}..+..~..+.....+.....+....'+....-+....<+....M+....V+....k+....x+....~+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....0,....[,....,.....,.....,.....,.....-.... -....#-
....$-....;-....\-....k-.....-.....-.....-.....-........!.6....:9....:l....:.....:!/...;./...;?0...;i0...;.0...;.0...;R1...;.1...;.1...;.1...;.2...;)3...;.3...;.3...;.3...;.3.. ;.4..#;.4..$;74..%;a4..&;.4..(;35..);.5..*;.5..+;.5
..,;.6..-;T6...;.6../;.7..0;.8..1;.:..2;(;..3;Y<..4;.<..5;.<..6;.=..7;\=..8;.>..9;.@..:;.A..;;.A..<;.A..=;.B..>;.C..@;.D..A;.E..C;hF..D;.F..E;.F..F;.F..G;.G..H;OG..I;fG..J;.G..L;.H..M;nI..N;
.J..O;.J..P;.J..Q;(K..R;.N..S;8P..T;.Q..U;0R..W;.R..Y;.R..Z;.R..[;.R..\;.R..];YS..b;uT..c;.T..d;.U..e;.U..f;5V..g;]V..h;:W..i;.W..j;.X..m;.Y..p;gY..q;.Y..r;.Y..s;.Y..t;.Y..u;.Y..v;
HZ..w;.Z..x;.Z..y;.Z..z;.Z..{;-[..|;][..};.[..~;.[...;.\...;%\...;H\...;O]...;.]...;R^...;.^...;.^...;._...;._...; _...;E_...;H_...;R_...;U_...;__...;b_...;p_...;t_...;._
```


C:\Users\user\AppData\Local\Programs\via\locales\ca.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	87098
Entropy (8bit):	5.431939868956806
Encrypted:	false
SSDEEP:	1536:XeBRevu71PR9GjMVNUqvnlluqcgKWI54FZn+O5yz8yLd9rXe0BU0dlszRh2h+nA7:mRevu71P3UqvnfXcgKWI54FZn+O5yz8y
MD5:	1D3F1900D6D59C680B25EF2AEBE75A15
SHA1:	4F8902494CA2FB2FD9C184840F84116A635B86E7
SHA-256:	527270623091F56A8A58A5474E016F70FFCF36498B02ED07C671912EDD457C66
SHA-512:	3D4A01713D31AD6CF92BA66C62E752F8971C84D04E29BE4D30F38FD3C5F9E464B15A2D11F6C49026752D12620687EA4A46D20F86605DC6A4642FF4C2071DD8C
Malicious:	false

Preview:


```
...........|..+..}..+..~.$+....,+....1+....>+....D+....S+....d+....m+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....+,....K,....f,.....,.....,.....,.....,.....,.....,....
.,.....,.....,.....,.....,.....,.....,.....-.....-.....-..!. -..".#-...:A-...:G-...:d-...:w-...;.-...;.-...;.-...;.....;.....;P....;s....;.....;.....;./...;W/...;./...;./...;./...;./.. ;./..#;./..$;./..%;./..&;.0..(;M0..);w0..*;.0..+;.0..,;
.0..-;.0...;.0../;d1..0;.1..1;k2..2;.2..3;.3..4;.3..5;.3..6;.3..7;.3..8;.4..:;X5..;;.5..<;.5..=;.5..>;.6..@;.7..A;.7..C;.8..D;.8..E;-8..F;98..G;I8..H;X8..I;n8..J;.8..L;.8..M;C9..N;.9..O;.9..
P;.9..Q;.9..R;.;..S;.;..T;.;..U;M<..W;}<..Y;.<..Z;.<..[;.<..\;.<..];.<..b;#=..c;T=..d;.=..e;.=..f;.=..g;*>..h;.>..i;.>..j;;?..m;m?..p;.?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.?..w;.@..x;.@..y;.@
..z;.@..{;L@..|;c@..};.@..~;.@...;.@...;.@...;.@...;TA...;.A...;.A...;.B...;2B...;BB...;FB...;QB...;YB...;\B...;gB...;jB...;tB...;wB...;.B...;.B...;.B
```


C:\Users\user\AppData\Local\Programs\via\locales\cs.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	88849
Entropy (8bit):	5.830130897775082
Encrypted:	false
SSDEEP:	1536:LtOEYhuIM85ryN1itrXljsDf1956h4ReO8Qi2rP:dN1ixXM5gJO8Qi2b
MD5:	C542E54EACD0A3105EB80D960A93F3FC
SHA1:	3C09CDB61B329F48025DBBC0FAF469E3208FE46C
SHA-256:	3C08DC65F95CCD0DCBEAB9BE148CF5F7632A6A01FC5B17A46518B8A48019D4AA
SHA-512:	7899A0F3296920C63567A9173895A0CA9F85E322A9B68E04834BA76070B2843A5FA1E0824FBAE078A4A082CAE9C0A7652BB49DBB10D717F0CF53E6D1466F3CFA
Malicious:	false

Preview:


```
...........|..+..}..+..~..+....&+....++....8+....>+....M+....^+....g+....|+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,.....,....&,....?,....T,....a,....n,....u,....},
.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:*-...:O-...:d-...;.-...;.-...;.-...;.-...;.-...;*....;=....;U....;c....;.....;./...;P/...;g/...;r/...;y/.. ;./..#;./..$;./..%;./..&;./..(;.0..);#0..*;60
..+;E0..,;K0..-;^0...;.0../;.0..0;O1..1;.1..2;82..3;.2..4;.2..5;.3..6;.3..7;23..8;.3..:;j4..;;.4..<;.4..=;.4..>;d5..@;.5..A;A6..C;.6..D;.6..E;.6..F;.6..G;.6..H;.6..I;.6..J;.7..L;H7..M;.7..N;
q8..O;.8..P;.8..Q;.8..R;.:..S;.;..T;q<..U;.<..W;.<..Y;.<..Z;.<..[;.<..\;.<..];%=..b;u=..c;.=..d;.>..e;.>..f;->..g;e>..h;.>..i;.>..j;G?..m;r?..p;.?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.?..w;.?..
x;.?..y;.@..z;.@..{;1@..|;G@..};.@..~;.@...;.@...;.@...;.@...;7A...;|A...;.A...;.A...;.B...;+B...;/B...;:B...;BB...;EB...;OB...;RB...;\B...;_B...;mB...;qB...;vB
```


C:\Users\user\AppData\Local\Programs\via\locales\da.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	80484
Entropy (8bit):	5.455533665728002
Encrypted:	false
SSDEEP:	1536:XqIilBBX9I/OaKuBMomQlq15+Z+GMyQ4wxpOmPvhw/j:XB+TX9yfoomQc15+ZoyWVw/j
MD5:	652136F8DEE3E802825E42C89BF0485C
SHA1:	307C6BCD9643BC059A04AA80E697A2F172C18AFF
SHA-256:	5698DC7D91C368FCACA23879F4DC50CB3979E606A154FC39840E3FA0DC702F18
SHA-512:	8B56B10E1A22061C846AA3B8C0EA30025F6C65E9594D42D70EB6E77B684200D35980F74E5D680C783919A6AD990ABB0E72E386A29FCF50A822626D7994BA2A3E
Malicious:	false

Preview:


```
...........|..+..}..+..~.*+....2+....7+....D+....J+....Y+....j+....s+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,.....,....0,....?,....X,...._,....h,....n,....q,
....x,....{,....|,.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:,...:,...:.-...:--..;T-...;.-...;.-...;.-...;.-...;.-...;.....;"....;,....;x....;.....;.....;.....;./...;./.. ;./..#;./..$;&/..%;:/..&;B/..(;./..);./..*;./..+;./..,;./..-
;./...;.0../;n0..0;.0..1;?1..2;.1..3;$2..4;62..5;X2..6;e2..7;v2..8;.2..9;.3..:;.3..;;.3..<;.4..=;N4..>;.4..@;D5..A;.5..C;.6..D;.6..E;'6..F;26..G;C6..H;R6..I;a6..J;o6..L;.6..M;.6..N;y7..
O;.7..P;.7..Q;.7..R;.8..S;b9..T;.9..U;%:..W;@:..Y;H:..Z;O:..[;V:..\;`:..];.:..b;.:..c;.;..d;y;..e;.;..f;.;..g;.;..h; <..i;e<..j;.<..m;.<..p;.=..r;.=..s;.=..t;.=..u;'=..v;==..w;O=..x;P=..y;^=..z;a=..{;
.=..|;.=..};.=..~;.=...;.=...;.>...;.>...;w>...;.>...;.>...;.?...;5?...;E?...;I?...;T?...;\?...;_?...;i?...;l?...;v?...;y?...;.?...;.?...;.?
```


C:\Users\user\AppData\Local\Programs\via\locales\de.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data

C:\Users\user\AppData\Local\Programs\via\locales\de.pak

Category:	dropped
Size (bytes):	86153
Entropy (8bit):	5.486586495316791
Encrypted:	false
SSDEEP:	1536:cAKB0+2BYlddBXgfnhryuYRmBYWfApJGHatP0Q1NlkG4hBlZOI80Ar5bN:xKS9KcryuYRm8GwbNqDZXA5bN
MD5:	E4055A9A8D1C64472281893943055328
SHA1:	2859CDC1658FA52A63138C5042091CBF8B91D48A
SHA-256:	82E57CF500D76CC7D2DF41034B1CDF73B1A498128CF598B3FB282B626EB58455
SHA-512:	8B7297595B8F878C24D93744B9F085A29B3808C81B1EBCEC0C86E6BE3AB9D91A46FFBF73A0585275E68F4FAD9E58073898BF7080036EB7666799A77F75CB7648
Malicious:	false

Preview:

............|..*..}..*..~..+.....+.....+.....+....$+....3+....D+....M+....b+....o+....u+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....4,....?,....K,....[,....e,
....l,....o,....p,....y,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:+-...:g-...:.-...;.-...;....;.....;....;5....;i....;{....;.....;.....;./...;i/...;./...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;H0..);h0..*;y0..+;.0..,;
.0..-;.0...;.0../;d1..0;.1..1;.2..2;I3..3;.4..4;.4..5;B4..6;S4..7;g4..8;.5..9;.5..:;.5..;; 6..<;C6..>;s6..A;"7..C;.7..D;.7..E;.7..F;.7..G;.7..H;.8..I;%8..J;A8..L;h8..M;.8..N;R9..O;Y9..P;d9..
Q;.9..R;.:..S;*;..T;.;..U;.<..W;0<..Y;9<..Z;G<..[;P<..\;_<..];.<..b;.<..c;.=..d;.=..e;.=..f;.=..g;.=..h;Q>..i;.>..j;.>..m;1?..p;_?..r;j?..s;o?..t;s?..u;.?..v;.?..w;.?..x;.?..y;.?..z;.?..{;.@
..|;.@..};R@..~;]@...;g@...;u@...;.@...;.A...;eA...;.A...;.A...;.A...;.A...;.A...;.A...;.B...;.B...;.B...;.B...;.B...;(B...;,B...;1B...;3B...;>B...;DB

C:\Users\user\AppData\Local\Programs\via\locales\el.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	148899
Entropy (8bit):	4.929242147484643
Encrypted:	false
SSDEEP:	3072:Npi9ixCcZ0pDFMlPDXPnUIgRPQpPQ2NSqi/EXMeELO+J9Kh52hKWPvYcGSS0zd:Npi9yCcgFIPDXvUIgRPQpPDHXMeF+Js4
MD5:	8B7C1D4A325B3CB33FA2DEDB965492E4
SHA1:	4FFEE3F95DD6C9C43B229500DD0515BEFA9E49C4
SHA-256:	E04C28635A79F0CCEB86FE471841E7B210A9D37137EC5D46A2E99893F64074C6
SHA-512:	C832F2C611023BA034D60F9088B984FCC9893BAA74C715B16B37C3AC8C5CA79437308BB07ECDA70BD31DC667C392815F2E35DF3941E56E52542EC8CB35C6A0
Malicious:	false

Preview:

............|..*..}..+..~..+.....+.....+....(+.....+....=+....N+....W+....l+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....h,.....,.....,.....,.....-.....-...."-....)-....,-
....--....@-....X-....`-....p-.....-.....-.....-.....-..!....."......:(....:I....:.....:.....;./...;./...;./...;.0...;!0...;.0...;.0...;.1...;!1...;.1...;.2...;.2...;.3...;03...;@3.. ;a3..#;u3..$;.3..%;.3..&;.3..(;g4..);.4..*;.4
..+;.4..,;.5..-;W5...;.5../;.6..0;.7..1;.8..2;.9..3;.:..4;.:..5;,;..6;S;..7;.;..8;.<..9;->..:;|>..;;.>..<;/?..>;.?..@;.@..A;}A..C;EB..D;hB..E;.B..F;.B..G;.B..H;.C..I;*C..J;NC..L;.C..M;.D..N;
GE..O;aE..P;.E..Q;.E..R;.G..S;.H..T;.I..U;%J..W;cJ..Y;qJ..Z;.J..[;.J..\;.J..];.K..b;.K..c;.K..d;.L..e;+M..f;LM..g;.M..h;.N..i; O..j;.O..m;>P..p;.P..q;.P..r;.P..s;.P..t;.P..u;.Q..v;
9Q..w;ZQ..x;[Q..y;zQ..z;}Q..{;.Q..|;.Q..};CR..~;RR...;hR...;~R...;.R...;oS...;.S...;IT...;.T...;.T...;.T...;.T...;.T...;.U...;.U...;.U...;.U...;.U...;"U...;0U...;4U...;XU

C:\Users\user\AppData\Local\Programs\via\locales\en-GB.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	72141
Entropy (8bit):	5.505693511311119
Encrypted:	false
SSDEEP:	1536:Y/+rWT2EpqqD4iRr595/BgSOQJedMPrThQzhfmgglQDD:YW02EpqOBBj5QQgglQP
MD5:	BC01EF9F07F4B7B43CA2BA68DBFAC1F3
SHA1:	24D98C278E569F6EA2E573E8ED34DA84F99699FD
SHA-256:	6710C03227C7053DBB5616244F0B35CFD1588BE005D547A0F023421530E1FE46
SHA-512:	917FC03D4DE29E231AEC3D03BD2A5A2862F65B6E920F6508E093761FC234CF964538DC28A199EE035A2A19C99D9C52E5FFEEA5C16531BC600E9351F1F1C1124
Malicious:	false

Preview:

............|..+..}..+..~.(+....0+....5+....B+....H+....W+....h+....q+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....(,....7,....H,....P,....X,...._,....d,
....k,....n,....o,....t,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:,...:,...:,...:.-...;,-...;`-...;k-...;u-...;z-...;.-...;.-...;.-...;.-...;.-...;(....;R....;c....;m....;r... ;....#;....$;....%;....&;....(;....);./..*;./..+;./..,;
./..-;-/...;Z/../;./..0;.0..1;l0..2;.0..3;11..4;@1..5;e1..6;q1..7;.1..8;.2..9;.2..:;.2..;;.2..<;.3..=;93..>;.3..@;.4..A;Y4..C;.4..D;.4..E;.4..F;.4..G;.4..H;.4..I;.4..J;.5..L;$5..M;.5..N;.5..
O;.5..P;.6..Q;.6..R;.7..S;.7..T;.7..U;!8..W;D8..Y;J8..Z;T8..[;[8..\;f8..];.8..b;.8..c;.8..d;89..e;L9..f;\9..g;.9..h;.9..i;.:..j;[:..m;.:..p;.:..q;.:..r;.:..s;.:..t;.:..u;.:..v;.:..w;.:..x;.:..y;.;..z;.;..{;';..
|;8;..};p;..~;w;...;{;...;.;...;.;...;.;...;)<...;N<...;o<...;.<...;.<...;.<...;.<...;.<...;.<...;.<...;.<...;.<...;.<

C:\Users\user\AppData\Local\Programs\via\locales\en-US.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	72950
Entropy (8bit):	5.4915925567870705
Encrypted:	false
SSDEEP:	1536:03l5u0fzEphzD2Vtrhm5uBpSOqJedMprphwnhfDgglgLFwd:03l5tzEphYFBMnwJgglghwd
MD5:	CE30D32061B772148CBC966915291EDC
SHA1:	4C5EDAED4F3BA6E10443F344E757C26F7CEB4CE9
SHA-256:	88A07BE1329CFDE3486DD0376DE77E289468A750273970AEAE6AD4468C0969F4
SHA-512:	720FA132A3362EA4F5EA10F30C4996378D1F196210CEF13C38579DBACC1F11E55D6DFDAA3AA0A6A574670A962F6E2910A2D66A64A1E7E1D6466B20529F5652C

C:\Users\user\AppData\Local\Programs\via\locales\en-US.pak	
Malicious:	false

Preview:

...........|..+..}.++..~.6+....>+....C+....P+....V+....e+....v+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....,.....,.....,.....,....&,....6,....E,....V,....^,....f,....m,....r,
....y,....|,....},.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:,...:,...:.-...:.-...;:-...;l-...;w-...;.-...;.-...;.-...;.-...;.-...;.-...;.....;/....;Y....;j....;s....;x... ;....#;....$;....%;....&;....(;....);./..*;./..+; /..,;$/..-
;3/...;\/../;./..0;.0..1;i0..2;.0..3;01..4;?1..5;d1..6;p1..7;.1..8;.2..9;.2..:;.2..;;.2..<;.3..=;:3..>;.3..@;.4..A;Z4..C;.4..D;.4..E;.4..F;.4..G;.4..H;.4..I;.4..J;.5..L;%5..M;.5..N;.5..O;.6..P;.6
..Q;'6..R;.7..S;.7..T;!8..U;R8..W;u8..Y;{8..Z;.8..[;.8..\;.8..];.8..b;.8..c;.9..d;i9..e;}9..f;.9..g;.9..h;.:..i;N:..j;.:..m;.:..p;.:..q;.:..r;.:..s;.:..t;.:..u;.;..v;.;..w;-;..x;.;..y;9;..z;<;..{;];..|;n;..};.;
..~;.;...;.;...;.;...;.;...;'<...;_<...;.<...;.<...;.<...;.<...;.<...;.<...;.<...;.<...;.<...;.=...;.=...;.=...;.=

C:\Users\user\AppData\Local\Programs\via\locales\es-419.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	85292
Entropy (8bit):	5.409494723372111
Encrypted:	false
SSDEEP:	1536:Zj4IfLaOV6SPZrKdg32LXGROuY8LK40KxFBMH5HhbPVfnDWu+:V4zE6SheEROXbf+
MD5:	FF816434D53EB3D8B6385D0ED3F2627E
SHA1:	00D7D4A0678818B42B1A8504E287C435CD423BAD
SHA-256:	717375F6C54FED018B23D08A2434E9055AD3AA14AA4C94633FF47706E2682492
SHA-512:	436A5266DF981E7F59943A43AEE4D68532BE646DF37D0E7FFD25F6F6C41F8301F58EF62AD0076199277775C5152B5F1737D70D3D4855F8D9833AFBE8284F787A
Malicious:	false

Preview:

...........|..+..}..+..~.&+.....+....3+....@+....F+....U+....f+....o+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....,....0,....J,....a,....j,....s,....|,.....,.....,....
.,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..-.."..-...:(-...:/-...:Q-...:b-...;.-...;.-...;.-...;.-...;.....;J....;l....;.....;.....;.....;H/...;}/...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;E0..);y0..*;.0..+;.0..,;.0..-;.0..
.;.0../;V1..0;.1..1;n2..2;.2..3;.3..4;.3..5;.3..6;.3..7;.4..8;.4..9;l5..:;.5..;;.5..<;.6..=;]6..>;.6..@;.7..A;.8..C;.8..D;.8..E;.8..F;.8..G;.8..H;.8..I;.8..J;.8..L;29..M;.9..N; :..O;(:..P;/:..Q;T:..R;
5;..S;.;..T;6<..U;.<..W;.<..Y;.<..Z;.<..[;.<..\;.<..];.=..b;Y=..c;.=..d;.=..e;.>..f;$>..g;U>..h;.>..i;.?..j;j?..m;.?..p;.?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.@..w;"@..x;#@..y;5@..z;8@..{;e@..
|;x@..};.@..~;.@...;.@...;.@...;.@...;mA...;.A...;.A...;=B...;vB...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B

C:\Users\user\AppData\Local\Programs\via\locales\es.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	86916
Entropy (8bit):	5.377960668037836
Encrypted:	false
SSDEEP:	1536:Z1RvPJg0EsLXwSlBLWftv9dY0FZvX9T3g42dh3B1h89zOKISx6ZNzY:Vvu0E4XwSbKI0sN8jgXM
MD5:	29E406A5E19A35A03825BBA2589EB757
SHA1:	E656709C79D4F90D0B695FB871D8C540C07B76BB
SHA-256:	922892EE19C2B5581DDD4EE277339D150576B5555920850B321D1CFF668879D6
SHA-512:	1BC3CEC78B13725C7274C8D44D8C192B37757E44A8C46DE1F41639D2D4278C04878E214E0A51DE047ADE315339387F3B0A58A121933B796F1B2CF8A010537B1D
Malicious:	false

Preview:

...........|..+..}..+..~..+....$+....)+....6+....<+....K+....\+....e+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....,....(,....B,....Z,....c,....l,....u,....{,....,....
.,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..-.."..-...:!-...:(-...:H-...:Y-...;{-...;.-...;.-...;.-...;.-...;%....;L....;u....;.....;.....;5/...;n/...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;=0..);q0..*;.0..+;.0..,;.0..-
;.0...;.0../;_1..0;.1..1;Y2..2;.2..3;i3..4;.3..5;.3..6;.3..7;.3..8;h4..9;.5..:;_5..<;.5..>;.5..A;m6..C;.6..D;.6..E;.6..F;.7..G;.7..H;!7..I;87..J;M7..L;.7..M;.7..N;W8..O;_8..P;q8..Q;.8..
R;.9..S;.:..T;.:..U;.:..W;.;..Y;.;..Z;.;..[;$;..\;4;..];b;..b;.;..c;.;..d;Q<..e;z<..f;.<..g;.<..h;K=..i;.=..j;.>..m;4>..p;g>..q;p>..r;y>..s;|>..t;.>..u;.>..v;.>..w;.>..x;.>..y;.>..z;.>..{;.?..|;.?..};
h?..~;p?...;v?...;.?...;.?...;.@...;]@...;.@...;.@...;.@...;.@...;.@...;.@...;.@...;.A...;.A...;.A...;.A...;"A...;&A...;-A...;/A...;?A...;DA

C:\Users\user\AppData\Local\Programs\via\locales\et.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	77466
Entropy (8bit):	5.501112766177588
Encrypted:	false
SSDEEP:	1536:kAaSgj1g3ZuB0oTD8bxQZNJl1zMECshfMfzpc:kpj12EB0ocxQZblVMCfUO
MD5:	E45987ADFDB4B7CE29A9B9167674C64A
SHA1:	65BCDEDC404A0B5A88B0159D126E9487C13C6094
SHA-256:	F5DD367864119091AFD657D7BF6E79CFBB5C3103910A379F64D55C0F936E4350
SHA-512:	B09E0CB7B331C7A21BABBEBA43169DE127814C40B790D40A89CF65E2FD1E388282BD6820177ED71C848EDE9CFAE152222E21398226A22D2A6F258A6193006D1A
Malicious:	false

Preview:

...........|..+..}.'+..~.2+....:+....?+....L+....R+....a+....r+....{+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....,....,....,....(,....=,....K,....a,....j,....t,....z,....,....,....
.,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:.-...:8-...:C-...;d-...;.-...;.-...;.-...;.-...;.-...;.....;.....;8....;.....;.....;./...;./...;!/...;(/.. ;7/..#;?/..$;E/..%;Z/..&;h/..(;./..);./..*;./..+;./..,;.0..-;.0..
.;J0../;.0..0;.1..1;.1..2;.1..3;.2..4;.2..5;.2..6;.2..7;.2..8;`3..:;.4..;;84..<;Z4..=;.4..>;.5..A;.5..C;.5..D;.6..E;.6..F;.6..G;$6..H;76..I;F6..J;_6..L;.6..M;.7..N;n7..O;~7..P;.7..Q;.7..R;.8
..S;!9..T;.9..U;.9..W;.9..Y;.9..Z;.9..[;.9..\;.:..];*:..b;u:..c;.:..d;.:..e;.;..f;";..g;S;..h;.;..i;.;..j;9<..m;U<..p;s<..r;z<..s;}<..t;.<..u;.<..v;.<..w;.<..x;.<..y;.<..z;.<..{;.=..|;)=..};S=..~;_=..
.;d=...;x=...;.=...;.=...;.>...;B>...;i>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>

C:\Users\user\AppData\Local\Programs\via\locales\fa.pak

C:\Users\user\AppData\Local\Programs\via\locales\fa.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	119827
Entropy (8bit):	5.217967842154896
Encrypted:	false
SSDEEP:	3072:6/kwXneRtqo6NN9/W2ESEmIsm0uKR2X6mA4OfRLEXIjEdr5Pea7E3oLAi4lnjmjx:EkwXneRtqo6NN9/W2ESEmJuY2X6mA4Oc
MD5:	099BF964BBEF722E4F3451BCB9FC9E8C
SHA1:	09C3D695E8747F6C45E19031E1BA57A9F27346F3
SHA-256:	72C1C51D997AD695213DE0FDCCFFCA768C419F78C82C6786B7295402C3E86B3C
SHA-512:	4966432AD117F3F041863896679A6BA4A4EEC53A7776F04D31DD00AA0C29B7A0C8798352F5BB26B3FB7208D0E680E334BBCE3AA5747320AFAF26A167F3461F14
Malicious:	false
Preview:	


```
............|..*..}..*..~..*.....*.....+.....+.....+....#+....4+....=+....R+...._+....e+....t+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....(,....H,....o,....,.....,.....,.....,.....,.....,....
.,.....,.....,.....,.....-....0-....C-....I-..!.\-..".._-...:}-...:.-...:.-...:.-...;5....;.....;.....;.....;.....;G/...;l/...;./...;./...;e0...;.0...;s1...;.1...;.1...;.1.. ;.1..#;.1..$;.1..%;.1..&;.2..(;.2..);.2..*;.2..+;.2..,;.2..-
;'3...;.3../;r4..0;G5..1;36..2;.7..3;.8..4;.8..5;_8..6;p8..7;.8..8;.9..:;.:..;;.;..<;B;..=;.;..>;n<..@;Z=..A;->..C;.?..D;.?..E;/?..F;I?..G;c?..H;{?..I;.?..J;.?..L;#@..M;.@..N;.A..O;.A..P;
.A..Q;"B..R;.D..S;.E..T;{F..U;.F..Y;.G..Z;4G..[;BG..\;YG..];.G..b;$H..c;{H..d;.I..e;3I..f;ZI..g;.I..h;$J..i;.J..j;"K..m;_K..p;.K..r;.K..s;.K..t;.K..u;.K..v;.L..w;-L..x;.L..y;NL..z;QL..{;.L..
|;.L..};.M..~;.M...; M...;2M...;HM...;.M...;WN...;.N...;.N...;.N...;.N...;.O...;.O...;.O...;.O...;)O...;,O...;<O...;?O...;MO...;UO...;]O...;`O...;jO...;tO...;.O
```


C:\Users\user\AppData\Local\Programs\via\locales\fi.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	79870
Entropy (8bit):	5.449865885662735
Encrypted:	false
SSDEEP:	1536:8OcgeavNb1d/c3JxHFI6q3v2CgUdJjKoR8dmmgxA1EuhUfOmg3:8O1hF5d/c3JxHdquCgUdJjNRwmmgx2rL
MD5:	691D5B048DDFDAAA705F8F6F6C689472
SHA1:	35710475CC745C8D1DEDE6ADF7B2027C9F0071A8
SHA-256:	20FD5702AD913EBA86BD6720C3B639852F28DC9FC1089536FD8AAA9BC3DFBCFA
SHA-512:	ECB582055AEC9DBAEB32A3978B5621B374C1063FA33F7FB6E175FBF20FBA9C7CAA7BC4B4B24BA619D0BD099BBC31DE2F2D5AAE5B0EFF1EFC8FB212D0105E3FDD
Malicious:	false
Preview:	


```
............|..*..}..*..~..+.....+.....+...."+....(+....7+....H+....Q+....f+....s+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....+,....D,....M,....U,....\,....a,
....h,....k,....l,....s,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:,...:.-...:*-...:@-...;h-...;.-...;.-...;.-...;.-...;.....;:....;I....;.....;./...;=/...;N/...;W/...;^/.. ;l/..#;t/..$;y/..%;./..&;./..(;./..);.0..*;.0
..+;,0..,;20..-;O0...;q0../;.0..0;B1..1;.1..2;.2..3;.2..4;.2..5;.2..6;.2..7;.3..8;.3..:;?4..;;l4..<;.4..=;.4..>;E5..A;.5..C;.6..D;$6..E;26..F;A6..G;R6..H;f6..I;x6..J;.6..L;.6..M;)7..N;.7..O;
.7..P;.7..Q;.7..R;.8..S;09..T;.9..U;.9..W;.9..Y;.9..Z;.:..[;.:..\;$:..];E:..b;.:..c;.:..d;.;..e;.;..f;%;..g;M;..h;.;..i;.;..j;*<..m;L<..p;v<..r;~<..s;.<..t;.<..u;.<..v;.<..w;.<..x;.<..y;.<..z;.<..{;.=
..|;'=..};e=..~;k=...;r=...;.=...;.=...;.>...;^>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.?...;.?...;.?...;.?...;!?...;%?...;+?...;-?...;;?
```


C:\Users\user\AppData\Local\Programs\via\locales\fil.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	88121
Entropy (8bit):	5.226141145438586
Encrypted:	false
SSDEEP:	1536:6XvGP/99OoiAhh0GeNvuNpEWnG/S4u+p4CzbeeQThlh01oNaFreMD:6fO/7OoiDuLCzqvsreW
MD5:	0EE8183ADFF71889F13192A0EEFC9D4D
SHA1:	E2623D51A8877C72CEE264DBC63BBA34980469A2
SHA-256:	2597B47A9A23DC358B42CBD9B7DDB161D48FF66BE9879B3CB07E60DB3B020EA8
SHA-512:	0D6A5C16DA76C5B9A2C2827548FA6858E3C3A8D15A9970351020F4E71A47F537A03E102AF50E7F42B8902B516265AEDC84DECE6ED57D8E652BFF0840B3FF38C
Malicious:	false
Preview:	


```
............|..+..}..+..~.&+.....+....3+....@+....F+....U+....f+....o+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....2,....E,....a,....i,....q,....|,.....,
.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..-.."..-...:$-...:6-...:^-...:y-...;.-...;.-...;.-...;.....;.....;?....;Q....;b....;j....;.....;./...;?/...;T/...;a/...;i/.. ;x/..#;~/..$;./..%;./..&;./..(;./..);.0..*;*0
..+;A0..,;I0..-;_0...;.0../;.0..0;g1..1;.1..2;\2..3;.2..4;.2..5;-3..6;E3..7;c3..8;.3..9;.4..:;.4..;;.5..<;45..=;e5..>;.5..@;h6..A;.6..C;C7..D;N7..E;]7..F;h7..G;|7..H;.7..I;.7..J;.7..L;.7..M;
[8..N;.8..O;.9..P;.9..Q;:9..R;.:..S;r;..T;.<..U;b<..W;.<..Y;.<..Z;.<..[;.<..\;.<..];.<..b;&=..c;P=..d;.=..e;.=..f;.=..g;.>..h;.>..i;.>..j;2?..m;Z?..p;.?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.?..
w;.?..x;.?..y;.@..z;.@..{;.@..|;G@..};.@..~;.@...;.@...;.@...;.@...;8A...;.A...;.A...;.A...;.B...;/B...;3B...;>B...;FB...;IB...;SB...;VB...;`B...;cB...;qB...;uB
```


C:\Users\user\AppData\Local\Programs\via\locales\fr.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	93269
Entropy (8bit):	5.401750126086286
Encrypted:	false
SSDEEP:	1536:TjndV0538UOcX9hGXEGXxDJlIzKudyroFruFcShuTjIWlotzMNLFUo:TTM538UOcX9hGXEGXxDJlIzKmyroFru8
MD5:	FBA102C2954366CDA831B61825BFC5B9

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\fr.pak</th></tr>
<tr><td>SHA1:</td><td>7CA0F9F1B7C8CBC7096BCE1784EDE0D02A19E136</td></tr>
<tr><td>SHA-256:</td><td>8980D3479F91C9E128866714D01DC95CCBAC8A6FC316E396419C39FC8A35D904</td></tr>
<tr><td>SHA-512:</td><td>8C9190D9E5230E57DB7ECF8630F607B872253988056CCEA693D7744B81FD2DA3DBECC9F187AF106FC44881D4F00EABEA87819D63C1DF446AD511A1A67DF7E2
5</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..+..}..+..~..+...."+....'+....4+....:+....I+....Z+....c+....x+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,.....,....5,....D,....L,....T,....],....c,....j,....
m,....n,....u,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:.-...:8-...:J-...;w-...;.-...;.-...;.-...;.-...;H....;a....;|....;.....;.....;./...;b/...;z/...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;60..);f0..*;x0..+;.0..,;.0..-
;.0...;.0../;{1..0;.2..1;.2..2;>3..3;.3..4;.4..5;+4..6;;4..7;V4..8;.4..9;.5..:;.5..;;-6..<;Q6..=;.6..>;37..A;.7..C;[8..D;k8..E;}8..F;.8..G;.8..H;.8..I;.8..J;.8..L;.9..M;.9..N;W:..O;j:..P;.:..Q;.:
..R;k<..S;<=..T;.=..U;A>..Y;m>..Z;.>..[;.>..\;.>..];.>..b;.?..c;J?..d;.?..e;.?..f;.?..g;&@..h;.@..i;.A..j;rA..m;.A..p;.A..q;.A..r;.A..s;.A..t;.A..u;.B..v;.B..w;$B..x;%B..y;<B..z;GB..{;uB..|;
.B..};.B..~;.B...;.B...;.B...;.C...;.C...;.C...;!D...;[D...;}D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\gu.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>167056</td></tr>
<tr><td>Entropy (8bit):</td><td>4.513426063689328</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:YKz2jxD3e81nAykRXpjdO3ZH6poYiBeI9CQDZKoOG+AuKkSHhSuKBYV27y1bU1Rk:XEiy9</td></tr>
<tr><td>MD5:</td><td>68A49C445261FBEE0A6D4884B1D274F8</td></tr>
<tr><td>SHA1:</td><td>A697183B26B948A615F3606DC5E22242841D9B88</td></tr>
<tr><td>SHA-256:</td><td>76AE556CC64E48F02AF7AA1F4701E7D3D305EFADEC8C59063006A99B550B891E</td></tr>
<tr><td>SHA-512:</td><td>96DCBE7BAE570F6BC3335DF13482A68519E7D53D62B404D546CBB8CE2170938A36C0F7DA0CAF2EEF805E6DC8853C1803C8BD0D527B83B72B3DF36A9ADD672
65</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..+..~..+.....+....!+.....+....4+....C+....T+....]+....r+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....;,....l,.....,.....,.....,.....-....+-....>-....E-....H-
....J-....a-.....-.....-.....-.....-.....-..........F...!.\..."._....:}....:.....:...../...;i/...;./...;./...;.0...;.0...;.0...;.0...;.0...;.1...;.1...;n2...;.2...;$3...;>3...;G3.. ;x3..#;.3..$;.3..%;.3..&;.3..(;.4..);.4..*;.4..+;
5..,;35..-;o5...;.5../;.7..0;.8..1;$9..2;-:..3;R;..4;.;..5;.;..6;.<..7;E<..8;.=..9;K?..:;.?..;;&@..<;o@..=;.@..>;.B..@;/C..A;7D..C;5E..D;VE..E;.E..F;.E..G;.E..H;.E..I;.F..J;RF..L;.F..M;
.H..N;(I..O;YI..P;yI..Q;.J..R;.M..S;.O..T;EP..U;.P..W;-Q..Y;=Q..Z;VQ..[;hQ..\;.Q..];.Q..b;.R..c;.R..d;.T..e;0T..f;bT..g;.T..h;.U..i;vV..j;-W..m;uW..p;.W..q;.W..r;.X..s;.X..t;#X..u;
rX..v;.X..w;$Y..x;%Y..y;TY..z;WY..{;.Y..|;.Y..};RZ..~;nZ...;.Z...;.Z...;.Z...;.[...;k\...;.\...;.]...;T]...;d]...;h]...;.]...;.]...;.]...;.]...;.]...;.]...;.]...;.]</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\he.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>104924</td></tr>
<tr><td>Entropy (8bit):</td><td>4.896708080395801</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:SZ/r8Ty+M3ZIzkE5I47XTpjUBcI/NJ1xnW:G/r8oIzkE5IwXTpjUBcI/NJ1xnW</td></tr>
<tr><td>MD5:</td><td>77D9D8DFAA23976617771FB312B1EE8A</td></tr>
<tr><td>SHA1:</td><td>7DA0108FA6FBF91E6CCA183BBFD405AC64A4442E</td></tr>
<tr><td>SHA-256:</td><td>A81CCB69AD2AB32EB10CD7DBCDFBE318967686858A11EAD2BF4E8D7E663CB203</td></tr>
<tr><td>SHA-512:</td><td>4D19A43F4E396BA8DC576AB7C48FAC28E9CCD100768FE8B9A226C7E9B8BBD7A75D00276D90F12794ED36489C4497874479A9E1624E88A00E7010D699354DD7D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..*..~..+.....+.....+...."+....(+....7+....H+....Q+....f+....s+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....%,....<,....Y,....a,....i,....q,....y,
.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,.....-..!..-.."..-...::-...:N-...:r-...:.-...;.-...;.-...;.-...;.....;#....;-....;j....;.....;.....;.....;^/...;./...;.0...;00...;=0...;G0.. ;\0..#;d0..$;l0..%;.0..&;.0..(;.1..);91..*;N1
..+;g1..,;o1..-;.1...;.1../;x2..0;.3..1;.3..2;Y4..3;.5..4;"5..5;T5..6;e5..7;.5..8;;6..9;*7..:;e7..;;.7..<;.7..=;*8..>;.8..@;.9..A;.:..C;.:..D;.:..E;.:..F;.:..G;.:..H;.;..I;&;..J;F;..L;.;..M;2<..N; =..
O;0=..P;L=..Q;|=..R;.@..S;6A..T;bB..U;.B..W;.B..Y;.B..Z;.C..[;.C..\;0C..];WC..b;.C..c;.C..d;YD..e;.D..f;.D..g;.D..h;aE..i;.E..j;.F..m;EF..p;.F..q;.F..r;.F..s;.F..t;.F..u;.F..v;.F..
w;.G..x;.G..y;.G..z;.G..{;UG..|;sG..};.G..~;.G...;.G...;.H...;.H...;.H...;.H...;3I...;qI...;.I...;.I...;.I...;.I...;.I...;.I...;.I...;.I...;.I...;.I...;.I...;.J</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\hi.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>171191</td></tr>
<tr><td>Entropy (8bit):</td><td>4.486041273387984</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:yULIG8AzwfKS53cWhxNq5Wo6ujTHef+a1oE3b8+LljYNh5/ChVmEQmKY4E6MZ/1Y:yUXSrs5</td></tr>
<tr><td>MD5:</td><td>50280F7269EB822C91857E18CE9525A8</td></tr>
<tr><td>SHA1:</td><td>95A0D6BAE3880B7395A37B788A7BC8BB27AD97D1</td></tr>
<tr><td>SHA-256:</td><td>5CA13AA5B79FED7EE31FC5755E346422714F5429C1E3C5444322CC6F27D6DB04</td></tr>
<tr><td>SHA-512:</td><td>721A16EC5275787A9817E54D449E03BDFCE0C9E9FE85A85D151BCC760DC9914BE5DEAA551CD1247DD7602D6D48A4AC1253539E45BD6116ED38B464F2EC2EF
F1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\hi.pak</th></tr>
<tr><td>Preview:</td><td>...........|..*..}..*..~..*.....+.....+.....+.....+....)+....:+....C+....X+....e+....k+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....@,....b,....,.....,.....,.....,.....-.....-.....-
.....-....D-....e-....q-.....-.....-.....-.....-........!....."."....:@....:d....:.....:.....;V/...;./...;./...;.0...;%0...;.0...;.0...;.1...; 1...;.1...;.2...;73...;h3...;.3...;.3.. ;.3..#;.3..$;.3..%;.4..&;04..(;.4..);55..*;e5
..+;.5..,;.5..-;.5...;n6../;e7..0;O8..1;d9..2;[:..3;};..4;.;..5;.;..6;.<..7;X<..8;.=..9;3?..:;x?..;;.?..<;.@..=;.@..>;.A..A;.B..C;.C..D;.C..E;.C..F;.C..G;.D..H;FD..I;dD..J;.D..L;AE..M;sF..N;
.G..O;.G..P;.G..Q;FH..R;5K..S;.L..T;.M..U;\N..W;.N..Y;.N..Z;.N..[;.N..\;.O..];.O..b;.P..c;>Q..d;1R..e;OR..f;.R..g;.R..h;.S..i;uT..j;;U..m;.U..p;9V..q;[V..r;zV..s;.V..t;.V..u;.V..v;
%W..w;{W..x;|W..y;.W..z;.W..{;yX..|;.X..~;/Y...;KY...;\Y...;.Y...;.Z...;9[...;.[...;.[...;+\...;;\...;?\...;J\...;c\...;f\...;p\...;s\...;}\...;.\...;.\...;.\...;.\...;.\</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\hr.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>84709</td></tr>
<tr><td>Entropy (8bit):</td><td>5.533851319755023</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:FbmV0KihKAvK7NPXtUDeQFBCXEyRWL8IilM5hnfvbQC26a1KCxQi:b/PKNXtUDeUCXEyEMMjnHbAf1KCxQi</td></tr>
<tr><td>MD5:</td><td>F3FF9859F4EBF45FAC7FFBDF20AEDA5B</td></tr>
<tr><td>SHA1:</td><td>90D350F390831CD3CA481CBE1C1F5D1320927A1D</td></tr>
<tr><td>SHA-256:</td><td>27D92843C2C4456DBEAF74BBA283746AD211CEE3CF8BCD52519363853BC2ECE8</td></tr>
<tr><td>SHA-512:</td><td>732991F13B6F4DB57C3279056C773E45DED828E2D1902F78A7D39379B3E8E3D1A3CC96C0E9EFAB0637FDD16481BF01D22816038A8A181E0A7CBC2105FE8C489</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..+..}.#+..~..+....6+....;+....H+....N+....]+....n+....w+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....,....,....,....,....,....(,....E,....V,....a,....m,....r,....y,....,....
.,....,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..,..".,,...:.-...:<-...:y-...:.-...;.-...;.....;4....;I....;P....;u....;.....;.....;.....;*/...;x/...;./...;./...;./...;./.. ;./..#;./..$;.0..%; 0..&;10..(;y0..);.0..*;.0..+;.0..,;.0..-
;.0...;.1../;.1..0;.1..1;Y2..2;.2..3;43..4;H3..5;i3..6;v3..7;.3..8;.4..9;.4..:;.4..;;*5..<;U5..=;.5..>;.6..@;u6..A;.6..C;97..D;D7..E;S7..F;\7..G;l7..H;.7..I;.7..J;.7..L;.7..M;]8..N;.9..
O;29..P;>9..Q;]9..R;Z;..S;K<..T;.=..U;_=..W;~=..Y;.=..Z;.=..[;.=..\;.=..];.=..b;.>..c;>>..d;.>..e;.>..f;.>..g;.>..h;Z?..i;.?..j;.?..m;(@..p;M@..r;T@..s;Z@..t;`@..u;x@..v;.@..w;.@..
x;.@..y;.@..z;.@..{;.@..|;.@..};1A..~;8A...;=A...;JA...;YA...;.A...;.B...;:B...;lB...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\hu.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>89863</td></tr>
<tr><td>Entropy (8bit):</td><td>5.664762851022001</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:flTMnDZAbpmFYkCFXmKLGqLv/Hu8nNhrZUoSd773dpE2jT/L5g3ICh:fKDZ0pmFYkCF2iGuv30d773dpE2jP5gb</td></tr>
<tr><td>MD5:</td><td>940FC7F16A7B112595A709814F91E57C</td></tr>
<tr><td>SHA1:</td><td>0C0064B701DEA3B1541652019DFAFF58F7AC3EB4</td></tr>
<tr><td>SHA-256:</td><td>85667D53EF4AD8FAA1492A134012557C433E076C1D27B3B3B1E4B2DD7B0AEABD</td></tr>
<tr><td>SHA-512:</td><td>83F9624FF34245065754C4A172346EAF924DD97D625229C19C2595AFE616DB89D82F6F27B17D4F483199C3BDA1A0E163034748BA40637189FF51216274883BA2</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..+..~..+.... +....%+....2+....8+....G+....X+....a+....v+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....',....<,....P,....],....j,....z,.....,.....,....
.,....,.....,.....,.....,.....,.....,.....,.....,.....-..!..-..".-...:/-...:C-...:t-...:.-...;.-...;.....;.....;8....;F....;.....;.....;.....;.....;0/...;./...;./...;./...;./...;./.. ;.0..#;.0..$;.0..%;.0..&;>0..(;.0..);.0..*;.0..+;.0..,;.0..-
;.0...;.1../;.1..0;.1..1;x2..2;.2..3;.3..4;.3..5;.3..6;.3..7;.3..8;.4..9;R5..:;.5..;;.5..<;.5..=;+6..>;.6..@;A7..A;.7..C;-8..D;F8..E;]8..F;m8..G;|8..H;.8..I;.8..J;.8..L;.8..M;.9..N;.9..O;.9..P;.:
..Q;':..R;@;..S;.;..T;/<..U;{<..W;.<..Y;.<..Z;.<..[;.<..\;.<..];.=..b;f=..c;.=..d;.=..e;">..f;7>..g;x>..h;.>..i;C?..j;.?..m;.?..p;.@..q;.@..r;(@..s;.@..t;1@..u;I@..v;d@..w;u@..x;v@
..y;.@..z;.@..{;.@..|;.@..};2A..~;9A...;EA...;UA...;eA...;.A...;%B...;VB...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.C</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\id.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>77956</td></tr>
<tr><td>Entropy (8bit):</td><td>5.382604957837571</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:oq7Hkraj/1Ze5/SWlEmCUwRX1EdtwbEB5g1CP5sAzb2VhwvRZQBcCaoJ:oqTMaj/1Ze5KWdtwbUZ5sAzaXwYBcCa6</td></tr>
<tr><td>MD5:</td><td>0A69835615E9445065C558DB76256ACC</td></tr>
<tr><td>SHA1:</td><td>E5031D6484EA686ED593223F893FF2B324429226</td></tr>
<tr><td>SHA-256:</td><td>1654D6BDDCE488E75829D790BC2392024227BFE7C88676006CE29BDB69E6E30C</td></tr>
<tr><td>SHA-512:</td><td>33FF0B82DB7350E80100687F7755D7124552CBB88209356B6894FD74EB2F415FD9820EC8202F4359A26439D55EC05BE64DD73AC8033779BF4EF9E5EEA7740757</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..*..~..+.....+.....+...."+....(+....7+....H+....Q+....f+....s+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,....,....*,....2,....:,....B,....G,
....N,....Q,....R,....X,....d,....j,....n,.....,.....,.....,.....,..!..,.."..,...:,...:,...:.-...:.-...;H-...;k-...;}-...;.-...;.-...;.-...;.-...;.-...;.-...;F....;.....;.....;.....;.....;.... ;....#;....$;....%;./..&;./..(;R/..);n/..*;|/
..+;./..,;./..-;./...;./../;L0..0;.0..1;!1..2;.1..3;.2..4;+2..5;I2..6;X2..7;{2..8;.3..9;.3..:;.3..;;.4..<;54..=;h4..>;.4..A;.5..C;.6..D;.6..E;.6..F;'6..G;>6..H;Q6..I;`6..J;r6..L;.6..M;.7..N;o7..O;.7..
P;.7..Q;.7..R;.8..S;.9..T;y9..U;.9..W;.9..Y;.9..Z;.9..[;.9..\;.:..];.:..b;\:..c;.:..d;.:..e;.:..f;.;..g;+;..h;.;..i;.;..j;.<..m;=<..p;i<..q;s<..r;}<..s;.<..t;.<..u;.<..v;.<..w;.<..x;.<..y;.<..z;.<..{;.=..|;!=..
};_=..~;n=...;r=...;.=...;.=...;.=...;0>...;S>...;t>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.></td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\it.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\it.pak</th></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>84595</td></tr>
<tr><td>Entropy (8bit):</td><td>5.318491727551267</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:6OHzYNl25Tmm0kfRIZY9f1t1Cz1yN4tA7kxAj4UNa79hnNOC:6IzF5Tmm0kfRIW9f1t1C5yN4tA7kxAji</td></tr>
<tr><td>MD5:</td><td>C83D309E006DED08A7C8951FE5217108</td></tr>
<tr><td>SHA1:</td><td>656D7EC9251BC9F3310E615561D1925A713821B2</td></tr>
<tr><td>SHA-256:</td><td>8CA6F63D7C826C8FABCC93F2665E4EC9950F799BE5FD9014BBDD3294C0F46652</td></tr>
<tr><td>SHA-512:</td><td>9FD15F281C9D5BEE80C371E83E04B570A9650C004F8FA42685514EDE3E04131BDF7C2187B123A8FD950743B03EFCFA0B289183B5DAF14B3A0E6BEA09E1856B1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..+..}..+..~."+....*+..../+....<+....B+....Q+....b+....k+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....1,....6,....G,....U,....`,....j,....p,
....w,....z,....{,....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:.-...:;-...:M-...;y-...;.-...;.-...;.-...;.-...;.....;3....;D....;L....;.....;.....;-/...;</...;E/...;M/.. ;f/..#;k/..$;s/..%;./..&;./..(;./..);.0..*;.0..+;
0..,;$0..-;@0...;{0../;.0..0;H1..1;.1..3;O2..4;l2..5;.2..6;.2..7;.2..8;]3..9;24..:;[4..;;.4..<;.4..=;.4..>;~5..@;.6..A;.6..C;.6..D;.7..E;.7..F;!7..G;37..H;C7..I;R7..J;l7..L;.7..M;.8..N;
.8..O;.8..P;.8..Q;.8..R;.9..S;u:..T;.:..U;C;..Y;i;..Z;|;..[;.;..\;.;..];.;..b;.;..c;0<..d;.<..e;.<..f;.<..g;.=..h;w=..i;.=..j; >..m;W>..p;.>..q;.>..r;.>..s;.>..t;.>..u;.>..v;.>..w;.>..x;.>..y;.>..z;.>..
{;.?..|;+?..};t?..~;~?...;.?...;.?...;.?...;.@...;b@...;.@...;.@...;.@...;.@...;.@...;.A...;.A...;.A...;.A...;.A...;"A...;%A...;3A...;7A...;<A...;>A</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\ja.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>102149</td></tr>
<tr><td>Entropy (8bit):</td><td>5.853654564506458</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:wZ02jh0ZHZ2BG3TLzWdSflHZcygvXUI4Zvx8HW6HvUFu9XBMh9++wizuNKVjrf:VDs+HblHZcHvlUm6h9+zizuNKV/</td></tr>
<tr><td>MD5:</td><td>B530E7114503306334F704268BB05ADE</td></tr>
<tr><td>SHA1:</td><td>CE2C039694AF6EBEBB2BC439FC6AB3A280DC6A53</td></tr>
<tr><td>SHA-256:</td><td>1C19D00E328C059D66C8CDBFF656A384C25145E6516C15EDBEB6E79A4C5E7726</td></tr>
<tr><td>SHA-512:</td><td>6E6A3F8F2C3F0B5E094FF1C3EA873F4B73346CAF16CB65A55F656874ADF817229385244716296B2474731E64694965DB6CC0D9E757EC0FF5323D61C40978F904</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>........~...|..*..}..*..~..*.....*.....*.....*.....*.....+.....+.....+....%+....++....=+....E+....J+....R+....]+....e+....t+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.... ,....),....2,....8,....A,....H,
....K,....X,....k,....q,....w,....},.....,.....,.....,..!..,.."..,...:,...:,...:.-...:7-...;s-...;.-...;.-...;.....;!....;`....;.....;.....;.....;D/...;./...;.0...;.0...;%0...;+0.. ;:0..#;@0..$;F0..%;g0..&;y0..(;.0..);.1..*;+1..
+;=1..,;C1..-;d1...;.1../;(2..0;.2..1;13..2;.3..3;R4..4;d4..5;.4..6;.4..7;.4..8;T5..:;%6..;;i6..<;.6..>;.6..A;z7..C;.7..D;.8..E;.8..F;68..G;T8..H;f8..I;w8..J;.8..L;.8..M;.9..N;.:..O;%:..P;7:
..Q;p:..R;[;..S;.;..T;.<..U;.<..W;.<..Y;.=..Z;.=..[;#=..\;5=..];o=..b;.=..c;.=..d;{>..e;.>..f;.>..g;.>..h;"?..i;p?..j;.?..m;.@..p;\@..r;b@..s;e@..t;h@..u;.@..v;.@..w;.@..x;.@..y;.@..z;.@..
{;'A..|;>A..};.A..~;.A...;.A...;.A...;.A...;XB...;.B...;.C...;UC...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.D...;.D...;.D...;.D</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\kn.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>191849</td></tr>
<tr><td>Entropy (8bit):</td><td>4.406706226377074</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:oVr7xJx7aipV8gTVNv4s18wEm3SF6RYNUTCKsy8/BS/27DSI:kr7xF8glEm3SF6RY2TCKsyP/27x</td></tr>
<tr><td>MD5:</td><td>1D6CD1093D3F5028ED2FBDAA67892AA5</td></tr>
<tr><td>SHA1:</td><td>C6CAC467DC2AF80BC3FF194A5A5005951D3FA7D0</td></tr>
<tr><td>SHA-256:</td><td>C1FF4D2E88EDBAAEEEDD05DB874F95387A6E58B2AD7CA86937B8E3D30197DD60</td></tr>
<tr><td>SHA-512:</td><td>0C90226C0B804FCA7FBD4AAAE184B66AAC721A9DC81BC58C69F155A5A54C2C13F0E549462CA7469854758D4524A08F400D44D3A389753731FAE3D7FD8578AEF
B</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..+..}..+..~..+....&+....++....8+....>+....M+....^+....g+....|+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....),....`,.....,.....,.....-....,-....P-....n-.....-.....-....
.-.....-.....-.....-.....-.....-....*.....e..............!....."......:.....:./...:}/...:./...;40...;.0...;.0...;M1...;e1...;.1...;,2...;.2...;.2...;r3...;.4...;.4...;.4...;.4...;.5.. ;-5..#;<5..$;Z5..%;.5..&;.5..(;[6..);.6..*;.6
..+;.7..,;F7..-;.7...; 8../;[9..0;_:..1;.;..2;.<..3;.=..4;$>..5;z>..6;.>..7;.?..8;.@..9;.B..:;.C..;;.C..<;.C..=;aD..>;.E..@;.F..A;.G..C;.H..D;.H..E;.I..F;8I..G;^I..H;.I..I;.I..J;.J..L;.J..M;
.K..N;2M..O;.M..P;.M..Q;.N..R;.R..S;.S..T;.U..U;.U..Y;3V..Z;sV..[;.V..\;.V..];1W..b;.X..c;.X..d;.Y..e;.Y..f;,Z..g;.Z..h;.[..i;.\..j;h]..m;.]..p;>^..q;Y^..r;t^..s;.^..t;.^..u;.^..v;A_..w;._..
x;._..y;._..z;._..{;._..|;.`..};.`..~;.`...;.`...;.a...;5a...;.b...;"c...;.c...;.c...;_d...;od...;sd...;~d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\ko.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>86324</td></tr>
<tr><td>Entropy (8bit):</td><td>6.165901109815054</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:cUnYAmztJhi1qVd7zd+7f25yTRQglxbEJALFwS2Q/4K5s4WGh/0S1zuyf:yAmJMqVd7z07f2wW2LF3/4KdW0/0S16+</td></tr>
<tr><td>MD5:</td><td>C3A5B2EAB6864263F06DEB21345CA9DA</td></tr>
<tr><td>SHA1:</td><td>676F07ACEA77952C7C2FD7B8BF979669E02B80FD</td></tr>
<tr><td>SHA-256:</td><td>2F1E11EFCCFD4540CFC6F3B089854987192E015B90AE50100C6862C9E4AFC2F8</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\via\locales\ko.pak	
SHA-512:	B6E1DA97F9D63C89CE936B9F46B0B0F567F407BD909ECCB8881A78C6BFFAA39A12C692CF7C54640323846C0A0CDE45A7922E7450591541E5F1919FEC172AB84
Malicious:	false
Preview:	

............|..*..}..*..~..*.....*.....*.....*.....*.....*.....+.....+...."+....1+....7+....I+....Q+....V+....^+....i+....q+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,.....,.....
',....-,....6,....L,....^,....k,....w,..!.~,.."..,...:,...:,...:,...:,...;.-...;c-...;.-...;.-...;.-...;.-...;.....;9....;E....;.....;.....;</...;O/...;j/...;s/.. ;./..#;./..$;./..%;./..&;./..(;.0..);@0..*;P0..+;]0..,;c0..-;.0
...;.0../;C1..0;.1..1;?2..2;.2..3;G3..4;^3..5;.3..6;.3..7;.3..8;T4..9;O5..:;.5..;;.5..<;.6..=;D6..>;.6..@;K7..A;.7..C;>8..D;R8..E;k8..F;.8..G;.8..H;.8..I;.8..J;.8..L;.9..M;.9..N;.9..O;.9..P;
.:..Q;.:..R;K;..S;.;..T;_<..U;.<..W;.<..Y;.<..Z;.<..[;.<..\;.=..];4=..b;.=..c;.=..d; >..e;D>..f;Q>..g;{>..h;.>..i; ?..j;y?..m;.?..p;.?..r;.?..s;.?..t;.?..u;.?..v;.@..w; @..x;!@..y;4@..z;7@..
{;l@..|;.@..};.@..~;.@...;.@...;.@...;.@...;gA...;.A...;.A...;0B...;bB...;rB...;vB...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B

C:\Users\user\AppData\Local\Programs\via\locales\lt.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	91387
Entropy (8bit):	5.627530738444946
Encrypted:	false
SSDEEP:	1536:WMHqr/DSTlZF5wxJDVOjWg00wsiYWdT9qKPrmzrfhli3xGm6SQ5njWSgAGiI6:WMKrLSTrwxJDQjET+BExGm6SQ5nD
MD5:	7A8EFD2DCAE15E8BB928A1602005CCBA
SHA1:	CA99BE66821A0C4664B213339C2829B1C02DE141
SHA-256:	D94EF525ABBC2625FDD7AE2DF30B947DBF3853F7ECB4D116754ED94C16804462
SHA-512:	2B980B9EC4B458B115CBFB650889AACEE4EF2C625276AAB3CF04C89035CF6DA3B89C8AB12C25D16CF6023E3BA6EC715640C03F0E84D0E6AD9F1CAB935E6F83C
Malicious:	false
Preview:	

............|..+..}..+..~..+....$+....)+....6+....<+....K+....\+....e+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....7,....H,....R,....],....d,....m,
....t,....w,....x,.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:3-...:`-...:z-...;.-...;.-...;.-...;.....;.....;@....;\....;x....;.....;.....;3/...;h/...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;70..);b0..*;u0
..+;.0..,;.0..-;.0...;.0../;Z1..0;.1..1;r2..2;.3..3;.3..4;.3..5;.3..6;.4..7;>4..8;.4..9;}5..:;.5..;;.5..<;.6..>;K6..A;.6..C;_7..D;l7..E;u7..F;.7..G;.7..H;.7..I;.7..J;.7..L;.8..M;.8..N;.9..O;.9..P;.9..
Q;.9..R;.<..S;I=..T;^>..U;.>..W;.>..Y;.>..Z;.>..[;.>..\;.?..];M?..b;.?..c;.?..d;,@..e;[@..f;r@..g;.@..h;.A..i;.A..j;.A..m;.B..p;GB..r;RB..s;XB..t;]B..u;uB..v;.B..w;.B..x;.B..y;.B..z;.B..{;.B
..|;.B..};+C..~;3C...;<C...;PC...;]C...;.C...;!D...;RD...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.D...;.E...;.E...;.E...;.E...;.E

C:\Users\user\AppData\Local\Programs\via\locales\lv.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	90503
Entropy (8bit):	5.64684607342749
Encrypted:	false
SSDEEP:	1536:Bol6UeSxXYGB5emD9iNyko6dZkmZa4WSun09hPpI02AM2fPy:AjXYGbCyko6dZkmZhvM2fPy
MD5:	DE31327F0843748A496A74A25F00BA22
SHA1:	DD94FFEA21EAD9CF0E538C271AAD1A15EED5731F
SHA-256:	2B9F8D694FE2FAE7444C9C05A0D15BCEFDFB37D78CE38E948C2584F32949E12C
SHA-512:	73A6EAE8A107B4F292E1B5C9A26726C85F4BBBF9368929E25BD0AD695CA0F0E0133E64AC9DE03EEFA002C10CF8AED81E3C91DF15C57F06430DE7988512C9484
Malicious:	false
Preview:	

............|..+..}.%+..~.0+....8+....=+....J+....P+...._+....p+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,.....,....*,....@,....[,....w,.....,.....,.....,.....,.....,.....
.,.....,.....,.....,.....,.....,.....,.....-.....-.....-..!.#-..".&-...:D-...:[-...:.-...:.-...;.-...;.-...;.....;.....;"....;U....;u....;.....;.....;.....;H/...;y/...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;>0..);h0..*;~0..+;.0..,;.0..-
;.0...;.0../;c1..0;.1..1;R2..2;.2..3;Q3..4;q3..5;.3..6;.3..7;.3..8;W4..9;!5..:;D5..;;r5..<;.5..=;.5..>;M6..@;.6..A;87..C;.7..D;.7..E;.7..F;.7..G;.7..H;.7..I;.8..J;-8..L;c8..M;.8..N;.9..
O;.9..P;.9..Q;.9..R;.;..S;.<..T;.=..U;.=..W;.>..Y;.>..Z;.>..[;*>..\;7>..];d>..b;.>..c;.>..d;0?..e;M?..f;b?..g;.?..h;.?..i;;@..j;.@..m;.@..p;.@..q;.@..r;.@..s;.@..t;.A..u;!A..v;7A..
w;^A..x;_A..y;uA..z;xA..{;.A..|;.A..};.A..~;.A...;.A...;.B...;(B...;.B...;.B...;.C...;MC...;vC...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C...;.C

C:\Users\user\AppData\Local\Programs\via\locales\ml.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	203423
Entropy (8bit):	4.4134685740425486
Encrypted:	false
SSDEEP:	1536:4drQH6H30ayc0qrelqBHa4KgdThKT9LhE3A86:4dQHAGc0qrexCdTwTjE3A86
MD5:	9E25E829DE22E617AE33D0F7DA21BF1F
SHA1:	F73B6C9D28EC3F5F00754CC23A6EE0BFE5D39C3C
SHA-256:	1CDB0CFFC941255A0A4911AA75996AB07F11C2E90237CFF9D429820550013228
SHA-512:	84F644F7BF15199D5C66167EEBE37FBE2A793CCFE0393BC6208C25783C63DF0C800C9EC81679184EAFFFEB7A077A3FD90C24CD997860164C9A9EC89D9A72AAF
Malicious:	false
Preview:	

............|..+..}..+..~..+...."+....'+....4+....:+....I+....Z+....c+....x+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....%,....k,.....,.....,.....-....C-....a-.....-.....-.....-.....-
.....-.....-..........*.....H.....i....................!../.."../...:8/...:W/...:./...:./...;G0...;.0...;.1...;&1...;J1...;.1...;/2...;h2...;.2...;.3...;.4...;45...;t5...;.5...;.5.. ;.5..#;.5..$;.6..%;56..&;i6..(;.7..);n7..*;.7
..+;.7..,;.8..-;V8...;.8../;#:..0;A;..1;.<..2;.=..3;M?..4;.?..5;.@..6;<@..7;.@..8;.B..9;JD..:;.D..;;"E..<;.E..=;.F..>;cG..@;.H..A;.I..C;.J..D;.K..E;3K..F;VK..G;.K..H;.K..I;.K..J;.L
..L;.L..M;.N..N;.O..O;uO..P;.O..Q;.P..R;.R..S;.S..T;.T..U;.U..W;.U..Y;.V..Z;:V..[;UV..\;.V..];.W..b;.X..c;.X..d;.Y..e;.Y..f;@Z..g;.Z..h;.[..i;k\..j;N]..m;.]..p;Z^..r;.^..s;.^..t;.^..u;.^..v;
;_..w;u_..x;v_..y;._..z;._..{;.`..|;=`..};.`..~;.`...;.a...;4a...;\a...;.b...;Lc...;.c...;=d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.d...;.e

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\mr.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>165740</td></tr>
<tr><td>Entropy (8bit):</td><td>4.503959880018125</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:nllbd+iIMN64Y5CWQ25H0c7epLtyWFQXSLQELBX5fOXDcIEf:CVe/Wq</td></tr>
<tr><td>MD5:</td><td>AC375F26E32FF3C17D65B0BA69A17B0D</td></tr>
<tr><td>SHA1:</td><td>47237085FE146905EAC156DD888187715E591E91</td></tr>
<tr><td>SHA-256:</td><td>3D2812B04004AC80946B2A466748A1CB405928DE26C2C5A3098444F234C22BEA</td></tr>
<tr><td>SHA-512:</td><td>3050F7A2C34A82AF57CBAF14E96751B123D58A1B44901783FE299DE2DB599BE73AA8AB76B352F452321FE556BF5B10624F68A96683064BC281D7CEF2A724E5A1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..*..~..+.....+.....+...."+....(+....7+....H+....Q+....f+....s+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.... ,....?,....g,....,....,....,....,.....-.....-.....-....!-
....#-....:-....W-....f-....u-.....-.....-.....-....%...!.;...".>....:\...:.....:./...:G/...;./...;g0...;.0...;.0...;.0...;31...;c1...;.1...;.1...;|2...;.3...;.3...;.3...;.3...;.3.. ;.4..#;14..$;J4..%;}4..&;.4..(;y5..
);.5..*;.5..+;36..,;O6..-;.6...;.7../;.8..0;.9..1;-:..2;';..3;Q<..4;.<..5;.<..6;.=..7;O=..8;.>..9;}@..:;.@..;;pA..<;.A..=;TB..>;.C..@;.D..A;.E..C;.F..D;.F..E;.F..F;.G..G;2G..H;uG..I;.G..J;.G
..L;JH..M;.I..N;.J..O;.J..P;.K..Q;]K..R;.M..S;.N..T;.O..U;.P..W;.P..Y;.P..Z;.P..[;.P..\;.P..];VQ..b;.R..c;rR..d;hS..e;.S..f;.S..g;aT..h;MU..i;.V..j;.V..m;JW..p;.W..q;.W..r;.W..s;.W
..t;.X..u;KX..v;.X..w;.X..x;.X..y;.X..z;.X..{;>Y..|;[Y..};.Z..~;.Z...;@Z...;WZ...;.Z...;i[...;.\...;m\...;.\...;.]...;+]...;/]...;:]...;B]...;E]...;O]...;R]...;\]...;_]...;m]...;q]</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\ms.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>79456</td></tr>
<tr><td>Entropy (8bit):</td><td>5.293673897835836</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:qKNpV6ScOkf6WQSWzCu2boe05DYOYxgudhRRWFD8u0CVf:a3OchWzCZoe051uPmd8u0Kf</td></tr>
<tr><td>MD5:</td><td>68EED78CFBED1F7D8EC60EF6D9DCA1FA</td></tr>
<tr><td>SHA1:</td><td>9DF230C4CCA8715B8BAD6351168DC47082D87FCE</td></tr>
<tr><td>SHA-256:</td><td>265D15D61FE5FB856E70D7FEFF9C1F5EB56336F012E88A3E907B5380B0A7527F</td></tr>
<tr><td>SHA-512:</td><td>531A35E49C0EF79B3F39D80C000F32700D259D89D623E2B07FD13527D04ADF70124E9ED513BFE937ACDDDCD0BE2C2D333BEB48492C72BC43E8BB2D3BA724A
2E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..+..~..+.....+.....+....*+....0+....?+....P+....Y+....n+....{+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....%,....2,....I,....S,....^,....f,....k,
....r,....u,....v,....|,....,....,....,....,....,....,....,..!..,.."..,...:.-...:.-...:/-...:E-...;q-...;.-...;.-...;.-...;.-...;.-...;....;$....;/....;....;....;....;./...;./...;&/.. ;7/..#;=/..$;E/..%;P/..&;Z/..(;./..);./..*;./..+;./..,;
./..-;.0...;,0../;.0..0;.0..1;p1..2;.1..3;Y2..4;j2..5;.2..6;.2..7;.2..8;23..9;.3..:;.4..;;04..<;P4..=;t4..>;.4..@;g5..A;.5..C;96..D;C6..E;P6..F;]6..G;t6..H;.6..I;.6..J;.6..L;.6..M;77..N;.7..
O;.7..P;.7..Q;.7..R;.8..S;L9..T;.9..U;.9..W;.:..Y;.:..Z;$:..[;-:..\;<:..];X:..b;.:..c;.:..d;.;..e;/;..f;>;..g;k;..h;.;..i;.<..j;d<..m;.<..p;.<..r;.<..s;.<..t;.<..u;.<..v;.<..w;.<..x;.<..y;.=..z;.=..{;
2=..|;G=..};.=..~;.=...;.=...;.=...;.=...;.>...;\>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.?...;.?...;.?...;.?...;'?...;+?...;.?</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\nb.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>78385</td></tr>
<tr><td>Entropy (8bit):</td><td>5.42825456747505</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:GwU9/1Gxlo/RNmKJz6BDNF6uImJMUvkhqCQ:GwU9tGvoZNmKYBDNF6uIMCY</td></tr>
<tr><td>MD5:</td><td>B95A6BE251B5011470A7D6F99914E45D</td></tr>
<tr><td>SHA1:</td><td>716078014B5109E74862E685F4074DC4E1A16F18</td></tr>
<tr><td>SHA-256:</td><td>21FA2E87F4C2142A5DE09DD42FA9A85D37BFD19E8B7FA10B960AE099CF613649</td></tr>
<tr><td>SHA-512:</td><td>F951AD557E3B76B7224188AD0ECFD05BE7B46F4758AB29F4C38A45D6A62D63E45ECBC811414CE32AC4AC55C2380BA90AC728172FC75ADFB7965C0596F49D40
F</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>...........|..*..}..+..~..+.....+....!+.....+....4+....C+....T+....]+....r+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....$,....;....B,....J,....U,....Y,....`,....
c,....d,....k,....v,....},....,....,....,....,....,....,..!..,.."..,...:,...:,...:.-...:*-...;X-...;.-...;.-...;.-...;.-...;.-...;....;3....;D....;....;....;./...;./...;$/...;+/.. ;>/..#;C/..$;K/..%;_/..&;k/..(;./..);./..*;./..+;./..,;./..-
;.0...;?0../;.0..0;#1..1;.1..2;.1..3;f2..4;y2..5;.2..6;.2..7;.2..8;+3..:;.3..;;.3..<;&4..>;W4..A;.4..C;*5..D;35..E;=5..F;I5..G;[5..H;k5..I;z5..J;.5..L;.5..M;#6..N;.6..O;.6..P;.6..Q;.6..
R;.7..S;.8..T;.8..U;.8..W;.8..Y;.8..Z;.8..[;.9..\;.9..];99..b;{9..c;.9..d; :..e;C:..f;V:..g;.:..h;.:..i;-;..j;|;..m;.;..p;.;..r;.;..s;.;..t;.;..u;.;..v;.<..w;#<..x;$<..y;3<..z;6<..{;b<..|;t<..};.<..~;.<...;.<..
.;.<...;.<...;W=...;.=...;.=...;.=...;.>...;%>...;)>...;4>...;<>...;?>...;I>...;L>...;V>...;Y>...;g>...;k>...;o>...;q>...;~>...;.></td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Programs\via\locales\nl.pak</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\via-1.3.1-win.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>82287</td></tr>
<tr><td>Entropy (8bit):</td><td>5.380337095761436</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:6Ks6wvW/ykDIwEyYn5tdU7A5k6m2Qwr1pHJ4hJo4TtpHQWozyVqf:6KqvW/awEyYn5td2A5kV2hDHJuu4TtpC</td></tr>
</table>

C:\Users\user\AppData\Local\Programs\via\locales\nl.pak

MD5:	A59A89C9979733AAC250850016251B30
SHA1:	B7EF504380295B114EC27369709FF15924F1316D
SHA-256:	B623917DABD97C7D5E506A76D57F29085FB017B82C7FE54F2E925F015A340445
SHA-512:	A55B6C6F350ABE6868CFDB1364E0437433460AF93930CCBEF25FC75F7DEBB0033C60BB1C61893D25845469490C5E19052554BFAAC092BA75AE846423CE2A259
Malicious:	false

Preview:

...........|..+..}..+..~."+....*+..../+....<+....B+....Q+....b+....k+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,.....,....),....;....O,....\,....i,....s,....z,.....,....
.,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:'-...:U-...:s-...;.-...;.-...;.-...;.-...;.....;K....;^....;p....;}....;.....;5/...;s/...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;.0..);*0..*;80..+;F0..,;L0..-
;b0...;.0../;.1..0;d1..1;.1..2;A2..3;.2..4;.2..5;.2..6;.3..7;.3..8;.3..9;M4..:;m4..;;.4..<;.4..=;.4..>;l5..@;.5..A;[6..C;.6..D;.6..E;.6..F;.6..G;.7..H;.7..I;%7..J;67..L;]7..M;.7..N;58..
O;F8..P;Q8..Q;r8..R;.9..S;.:..T;y:..U;.:..W;.:..Y;.:..Z;.:..[;.;..\;.;..];=;..b;~;..c;.;..d;)<..e;D<..f;X<..g;.<..h;.<..i;&=..j;m=..m;.=..p;.=..q;.=..r;.=..s;.=..t;.=..u;.>..v;.>..w;/>..x;0>..y;;>..z;
>>..{;h>..|;.>..};.>..~;.>...;.>...;.>...;.>...;p?...;.?...;.?...;.?...;.@...;-@...;1@...;<@...;D@...;G@...;Q@...;T@...;^@...;a@...;o@...;s@

C:\Users\user\AppData\Local\Programs\via\locales\pl.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	88465
Entropy (8bit):	5.748138223488504
Encrypted:	false
SSDEEP:	1536:b891hURMa8od+txCoqn6rIaC47gsN+hDiVAhYh:0RtxCoq4a4ZcDiV/
MD5:	CA1620E4BDC407C566F6F40572BC88C4
SHA1:	8AE22A47A39C7F1036F86367B10AAA493A9F9F82
SHA-256:	B2A2218CB02861946385BB6482BA8F869553DE86DC43D36532D7B61B9CB1779A
SHA-512:	A63E11162865EDBE6A48967D66F650C9301CA161E84E6A3A42BE119BE94580F57CF7A4A8C76A51BCD3CC605895EC3554ECA768690C542DD96675049B7E93717
Malicious:	false

Preview:

...........|..+..}..+..~.$+....,+....1+....>+....D+....S+....d+....m+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,.....,....*,..../,....D,....O,....[,....e,....l,
....s,....v,....w,....~,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:.-...:H-...:e-...;.-...;.-...;.-...;.....;.....;=....;Z....;z....;.....;.....;//...;h/...;}/...;./...;./.. ;./..$;./..%;./..&;./..(;.0..);:0..*;I0..+;[0
..,;a0..-;z0...;.0../; 1..0;.1..1;.2..2;z2..3;.3..4;*3..5;^3..6;o3..7;.3..8;.3..:;.4..;;.4..<;.4..=;.5..>;.5..@;(6..A;.6..C;.6..D;.7..E;.7..F;.7..G;&7..H;:7..I;J7..J;\7..L;.7..M;.8..N;.8..O;
.8..P;.8..Q;.8..R;.:..S;.;..T;s<..U;.<..W;.<..Y;.<..Z;.<..[;.<..\;.=..];&=..b;g=..c;.=..d;.=..e;.>..f;.>..g;B>..h;.>..i;.>..j;.?..m;V?..p;~?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.?..w;.?..x;.?..y;.?..z;.@
..{;(@..|;=@..};z@..~;.@...;.@...;.@...;.@...;.A...;cA...;.A...;.A...;.A...;.A...;.A...;.A...;.B...;.B...;.B...;.B...;.B...;"B...;0B...;4B...;9B...;;B

C:\Users\user\AppData\Local\Programs\via\locales\pt-BR.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	84446
Entropy (8bit):	5.453285986219093
Encrypted:	false
SSDEEP:	1536:vmrYBr2LL6GeOStVY0KzMQN0Y0X4Y5hec6x0xGUX4DbMB9P5ZC:vmkNY+JOStmMQzowMB9C
MD5:	603057CA797BE5E293FD9B02AE4D7AC1
SHA1:	D8358ADA4997FD5758652052D68F52220F1BF90C
SHA-256:	2D6007DE3EC09819554D6209724A7494CD8D68459AF3EC841789F57934CD266D
SHA-512:	DE32D40B09F6876F0259CCDC10A59B04810B424F299F610B3649D9897ACC42932C6B803FF0A34F362D7143AB634F927E456903F9F87B7CC8B22A1C319689F2EF
Malicious:	false

Preview:

...........|..+..}..+..~..+....&+....++....8+....>+....M+....^+....g+....|+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....,.....,....5,....M,....b,....k,....t,....},.....,
....,.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..,.."..,...:.-...:.-...:<-...:L-...;u-...;.-...;.-...;.-...;.-...;.....;.....;'....;1....;.....;.....;./...;./...;!/...;)/.. ;?/..#;E/..$;N/..%;]/..&;k/..(;./..);./..*;./..+;./..,;./..-
;.0...;L0../;.0..0;*1..1;.1..2;&2..3;.2..4;.2..5;.2..6;.2..7;.3..8;.3..9;.4..:;.4..;;.4..<;.5..=;?5..>;.5..@;K6..A;.6..C;(7..D;67..E;D7..F;R7..G;`7..H;r7..I;.7..J;.7..L;.7..M;;8..N;.8..
O;.8..P;.8..Q;.8..R;.:..S;E;..T;.;..U;B<..W;h<..Y;p<..Z;|<..[;.<..\;.<..];.<..b;.<..c;+=..d;.=..e;.=..f;.=..g;.=..h;H>..i;.>..j;.>..m;$?..p;U?..r;^?..s;b?..t;e?..u;{?..v;.?..w;.?..x;.?..y;.?
..z;.?..{;.?..|;.?..};C@..~;M@...;S@...;`@...;r@...;.@...;2A...;_A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.A...;.B

C:\Users\user\AppData\Local\Programs\via\locales\pt-PT.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	84703
Entropy (8bit):	5.439652497953441
Encrypted:	false
SSDEEP:	1536:L+HpED1EsYCBeWdRhVxz2qKHxpeJKWWYCx/:LsEDusYN4bJKWRC5
MD5:	35A7AA99B69432D295F9C64A2C16E4F9
SHA1:	91D9EB88378CF620B1D21F5E647E2A715277513A
SHA-256:	861E467DDD65915B6BE5E0F4EDDB8D67546AFCC798D34F7A6B6E079B671904DB
SHA-512:	42656DE8819692B87937038F116A2A8A105C17D5997CD18F21B0683D824AAB2251AF69152797B6AB498A588A764B3EECD5701D55BBBA72F307B3F424C569FC43
Malicious:	false

C:\Users\user\AppData\Local\Programs\via\locales\pt-PT.pak

Preview:

............|..+..}..+..~.*+....2+....7+....D+....J+....Y+....j+....s+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....",....7,....R,....d,....m,....v,.....,.....,
....,.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..,..".,...:.-...:#-...:D-...:T-...;}-...;.-...;.-...;.-...;.-...;*....;D....;e....;o....;.....;"/...;^/...;v/...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;&0..);Q0..*;a0
..+;o0..,;y0..-;.0...;.0../;@1..0;.1..1;22..2;.2..3;43..4;N3..5;{3..6;.3..7;.3..8;M4..9;$5..:;Q5..;;.5..<;.5..=;.5..>;x6..@;.6..A;o7..C;.7..D;.7..E;.7..F;.8..G;.8..H;18..I;H8..J;`8..L;.8..M;
.9..N;.9..O;.9..P;.9..Q;.9..R;.:..S;t;..T;.;..U;=<..W;d<..Y;l<..Z;x<..[;.<..\;.<..];.<..b;.=..c;S=..d;.=..e;.=..f;.=..g;/>..h;.>..i;.>..j;'?..m;h?..p;.?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.?..w;.?..x;.?
..y;.@..z;.@..{;=@..|;U@..};.@..~;.@...;.@...;.@...;.@...;VA...;.A...;.A...;.B...;/B...;?B...;CB...;NB...;VB...;YB...;cB...;fB...;pB...;sB...;.B...;.B

C:\Users\user\AppData\Local\Programs\via\locales\ro.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	87484
Entropy (8bit):	5.473143034921812
Encrypted:	false
SSDEEP:	1536:BrMkVL7qczyp6KvtGTMXjcQb0NnobyVwbEYu2zwpgSlJt/hYAh6qIbp92G4f6:N2cGp1vtGQwQbSYu2nSXYAh6qINkGP
MD5:	6DDB918017D8453646C347E1C7F10E8A
SHA1:	7F7C648940134EF5A8C1B2237E206A74FADDB5EF
SHA-256:	275745D81DAC9FBD35D57342E8F9790CF32C3984133C826F1AB5C9A9E8242916
SHA-512:	37403EF9B8AC5D99D74DB7A07C98E8E4BFC27A2E7273017C08448CAB64DF00A34BFE15D24BFD94C5A5B0FBE061C95F235D6BCAAB77C9B8B7494CF2C978657E DD
Malicious:	false

Preview:

............|..+..}.%+..~.0+....8+....=+....J+....P+...._+....p+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,.....,.....,.....,.....,....-,....C,....U,....a,....m,....z,.....,
....,.....,.....,.....,.....,.....,.....,.....,.....,.....,.....,..!..-.".-..:#-...:8-...:k-...:.-...;.-...;"....;3....;H....;M....;}....;.....;.....;.....;./...;b/...;./...;./...;./...;./.. ;./..#;./..$;./..%;./..&;.0..(;W0..);x0..*;.0
..+;.0..,;.0..-;.0...;.0../;^1..0;.1..1;>2..2;.2..3;.3..4;B3..5;k3..6;{3..7;.3..8;.4..9;.4..:;.4..;;.5..<;.5..=;Z5..>;.5..@;Q6..A;.6..C;.7..D;&7..E;.7..F;97..G;G7..H;^7..I;n7..J;.7..L;.7..M;-
8..N;.8..O;.8..P;.8..Q;.8..R;X:..S;.;..T;.;..U;.;..Y;.<..Z;.<..[;.<..\;-<..];W<..b;.<..c;.<..d;3=..e;N=..f;^=..g;.=..h;.=..i;.>..j;.>..m;.>..p;.>..r;.>..s;.>..t;.>..u;.>..v;.?..w;,?..x;-?..y;A?..z;D?
..{;l?..|;.?..};.?..~;.?...;.?...;.?...;.@...;.@...;.@...;.@...;.A...;6A...;FA...;JA...;UA...;]A...;`A...;jA...;mA...;wA...;zA...;.A...;.A...;.A...;.A

C:\Users\user\AppData\Local\Programs\via\locales\ru.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	134331
Entropy (8bit):	5.043966137383374
Encrypted:	false
SSDEEP:	3072:210reY9B95Sv5W+2pitEoDQgIvR7wAvrt3t2bqaPzLt3mV7Lle9X+vT042Z4Rkxr:MtcHHTqtDQgIvuAvhd2Zvt3mBoF404Kd
MD5:	26E967E4E67D58D22DAA45B0511945E7
SHA1:	C5917EA76641EA1F1395C12A29B036A2C57A5C0B
SHA-256:	6B1226AA78EE841552A8B2F22EE33B73778A94B835232522AAA66D73122E73A9
SHA-512:	4D2EEFD0CE55C01659D98BD2B0F88970DB4F4847684C1DF3D157164E0228D1B40F9FDD2C43C0B037689B900E77D80E70CDDFA8C22087A5DAD2D01DAD02222D 9
Malicious:	false

Preview:

............|..*..}..*..~..*.....*.....*.....+.....+.....+....(+....1+....F+....S+....Y+....h+....n+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....<,....c,....s,.....,.....,.....,.....,.....
.,.....,.....,.....,.....,.....,.....-....@-....Q-....]-..!.v-..".y-...:.-...:.-...;.-...;{....;.....;.....;./...;-/...;]/...;w/...;+0...;.0...;.1...;21...;O1...;]1.. ;z1..#;.1..$;.1..%;.1..&;.1..(;G2..);.2..*;.2..+;.2..,;.2..-;.2
...;*3../;34..0;.4..1;.5..2;Y6..3;A7..4;e7..5;.7..6;.7..7;.7..8;.8..:;(:..;;v:..<;.:..C;.:..D;.;..F;.;..G;0;..H;\;..I;u;..J;.;..L;.;..M;.<..N;.>..O;.>..P;5>..Q;.>..R;.B..S;.C..T;IE..U;.E..Y;.E..Z;.E..
[;.F..\;5F..];wF..b;.G..c;AG..d;.G..e;.H..f;?H..g;.H..h;.I..i;vI..j;.J..m;XJ..p;.J..r;.J..s;.J..t;.J..u;.J..v;.K..w;JK..x;KK..y;~K..z;.K..{;.K..|;.K..};IL...;ZL...;iL...;.L...;.L...;kM...;.M...;.M...;
.M...;.N...;.N...;.N...;%N...;(N...;2N...;5N...;?N...;EN...;SN...;WN...;aN...;cN...;kN...;uN...;.N...;.N...;.N...;.N...;.N...;.N...;.O

C:\Users\user\AppData\Local\Programs\via\locales\sk.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	89621
Entropy (8bit):	5.79426609462712
Encrypted:	false
SSDEEP:	1536:BMvqW9E7u3bevBTQEUcYaQ/QIRvZhRNwoqcHCYnpnGeP3g7E:DRqCBTQE6aQ/J7RNwoqcHCYnJGePg7E
MD5:	014ACAA7678B5351A06ACB8B0B9B205B
SHA1:	C5D4B4C5054973C290A4263EC455ED795C1EB0B8
SHA-256:	8BE2FB8EE246D879F929C0A3CB1AE725AFA74B0F1D241EB5579BCF5EE990EE50
SHA-512:	6505E6A5C0F00CABD31BED4DECF59F26845BDEB383EA5F73A48A827933509AF02EEC8E703B802C71DFBB305F22BEFF0B8E934B4253415AD71205299559C8BB5 E
Malicious:	false

Preview:

............|..+..}.%+..~.0+....8+....=+....J+....P+...._+....p+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,.....,.... ,....2,....L,....a,....o,....},.....,.....,.....,....
.,.....,.....,.....,.....,.....,.....,.....,.....,.....-..!..-."..-...:--...:?-...:d-...:z-...;.-...;.-...;.....;.....;.....;K....;`....;|....;.....;.....;=/...;x/...;./...;./...;./.. ;./..#;./..$;./..%;./..&;./..(;=0..);d0..*;x0..+;.0..,;.0..-
;.0...;.0../;a1..0;.1..1;?2..2;.2..3;)3..4;>3..5;e3..6;t3..7;.3..8;!4..9;.4..:;.5..;;A5..<;g5..=;.5..>;.6..C;.6..D;.6..E;.6..F;.6..G;.6..H;.6..I;.6..J;.6..L;37..M;.7..N;d8..O;z8..P;.8..Q;.8..R;.:
..S;.;..T;f<..U;.<..W;.<..Y;.<..Z;.<..[;.<..\;.<..];%=..b;.=..c;.=..d;.>..e;/>..f;=>..g;u>..h;.>..i;.?..j;d?..m;.?..p;.?..q;.?..r;.?..s;.?..t;.?..u;.?..v;.@..w;.@..x;.@..y;/@..z;2@..{;r@..|;
.@..};.@..~;.@...;.@...;.@...;.@...;uA...;.A...;.B...;=B...;oB...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B...;.B

C:\Users\user\AppData\Local\Programs\via\locales\sl.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	85805
Entropy (8bit):	5.5026219426420075
Encrypted:	false
SSDEEP:	1536:a3O8KEgw/qvkiNxnIOO43g9av9M/JdFCOoOqghxGTTXUtfpqG:a+mWkOnIc3qqM7FCOTxGTTXEfpqG
MD5:	3F352FD2B6D628E729761F66A1127EF6
SHA1:	16D5D482FDB4CE722BC1CA00C405C58F398AFB25
SHA-256:	E91835FE1D9F93E8E0E08B1A08392B7FE1E8716B4712DF5BA6E7D208AA60F6D6
SHA-512:	2F33DE72FA8E762C0968DBB0B13DC9BB5A9F1AEDA9CDA5836145421B32A3CAD424767EA81843420E8273D37B5C3379A65038F14A4D0303CE6F6CD14CA3A0BCBC
Malicious:	false
Preview:	

...........|..*..}..*..~..+.....+.....+....$+....*+....9+....J+....S+....h+....u+....{+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....&,....9,....C,....K,....Q,....V,
....],....`,....a,....i,....t,....y,.....,.....,.....,.....,.....,..!..,..".,...:,...:,...:.-...:0-...;]-...;.-...;.-...;.-...;.-...;.....;8....;[....;h....;.....;./...;>/...;S/...;\/...;c/.. ;./..$;./..%;./..&;./..(;./..);.0..*;.0..+;@0
..,;H0..-;c0...;.0../;.0..0;c1..1;.1..2;Q2..3;.2..4;.2..5;.3..6;.3..7;03..8;.3..9;34..:;_4..;;.4..<;.4..=;.4..>;{5..@;.5..A;i6..C;.6..D;.6..E;.6..F;.6..G;.6..H;.7..I;!7..J;87..L;k7..M;.7..N;
.8..O;.8..P;.8..Q;.9..R;.;..S;.<..T;.=..U;.=..W;.>..Y;.>..Z;.>..[;.>..\;2>..];R>..b;.>..c;.>..d;.?..e;#?..f;6?..g;p?..h;.?..i;.@..j;P@..m;p@..p;.@..q;.@..r;.@..s;.@..t;.@..u;.@..v;
.@..w;.@..x;.@..y;.@..z;.@..{;(A..|;=A..};yA..~;.A...;.A...;.A...;.A...;.B...;ZB...;.B...;.B...;.B...;.B...;.C...;.C...;.C...;.C...;.C...;#C...;&C...;4C...;8C...;?C

C:\Users\user\AppData\Local\Programs\via\locales\sr.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	128600
Entropy (8bit):	4.966396411786665
Encrypted:	false
SSDEEP:	3072:UJQwY2ptCOFiNJsMwy1Y+tZD+37hbVO08n9AU+Nlt3r1GL9DGk1XlE:Co+iUSLZS37hZOl9AdFk1u
MD5:	0497B7130484A365753EC331248D2B19
SHA1:	A0509FE81F6653DADCC6C263DB21884296364276
SHA-256:	FA010563901BB84272C15A71A4D80118B8FF22F4D5ABC8E4EF0314C00EB5F037
SHA-512:	8451E29832DC0122F46A21EB57185F545153A14CEAED421D4511FBB9BA316B7C139CF7CDCB8930064D577AB2D651051442C8545D072209DDD00415D7F37E2664
Malicious:	false
Preview:	

...........|..+..}..+..~.*+....2+....7+....D+....J+....Y+....j+....s+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+....(,....K,....p,.....,.....,.....,.....,.....,.....-.....-.....-
.....-....$-....:-....D-....T-....m-.....-.....-.....-..!..-..".-...:.-...:.....:B....:g....;.....;./...;C/...;./...;./...;.0...;_0...;x0...;.1...;.1...;.1...;.2...;.2...;-2.. ;M2..#;[2..$;m2..%;.2..&;.2..(;=3..);.3..*;.3..+;.3
..,;.3..-;.4...;p4../;.5..0;.5..1;.6..2;+7..3;.7..4;.8..5;F8..6;_8..7;.8..8;D9..:;O:..;;.:..<;.:..>;^;..A;.<..C;.<..D;.<..E;.<..F;.<..G;.<..H;.=..I;3=..J;V=..L;.=..M;.>..N;.?..O;.?..P;.?..Q;
.@..R;-C..S;fD..T;.E..U;AF..W;vF..Y;.F..Z;.F..[;.F..\;.F..];.G..b;nG..c;.G..d;`H..e;.H..f;.H..g;.H..h;.I..i;.J..j;.J..m;.J..p;.J..q;.K..r;.K..s;(K..t;4K..u;]K..v;.K..w;.K..x;.K..y;.K..z;.K..
{;.L..|;4L..};.L..~;.L...;.L...;.L...;.L...;.M...;.N...;SN...;.N...;.N...;.O...;.O...;.O...;.O...;.O...;&O...;)O...;3O...;6O...;DO...;HO...;VO...;XO...;dO...;pO

C:\Users\user\AppData\Local\Programs\via\locales\sv.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	78213
Entropy (8bit):	5.535774584296557
Encrypted:	false
SSDEEP:	1536:Y48CmEDTaCxiVeSynzyEy1d3bIkcWpdP/ldOZnCMqeLGBqTP+bRAplEFwSM/ymh6:Y4Vm8aCxiVLynz+cGby+qOx
MD5:	ED3B9C5064E1453444B5A2649EAD4076
SHA1:	BE64B48BACAA81004903719AE0A9A078887D10E1
SHA-256:	3A6746E9A6B609557B7A872AD1132907F6BDDC0B9AE22BBD05E79D2BA42D95AA
SHA-512:	8AEFC77C4B64EDA81539691A0B4E69A13ED63AB3BB62F644AEF6F8BEB0707EDDF59C3E9927EA2FAED943E475454978184CF28F42744034220F29CC5646F6FBC4
Malicious:	false
Preview:	

...........|..+..}..+..~..+...."+....'+....4+....:+....I+....Z+....c+....x+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....%,....5,....I,....Q,....Y,....d,....j,
....q,....t,....u,....},.....,.....,.....,.....,.....,.....,.....,..!..,..".,...:,...:,...:.-...:--...;_-...;.-...;.-...;.-...;.-...;.-...;.....;/....;:....;.....;.....;./...;./...;./...;./.. ;1/..#;6/..$;?/..%;T/..&;`/..(;./..);./..*;./..+;./..,;./..-
;.0...;;0../;.0..0;.1..1;u1..2;.1..3;`2..4;w2..5;.2..6;.2..7;.2..8;I3..9;.3..:;!4..;;[4..<;.4..>;.4..A;85..C;.5..D;.5..E;.5..F;.5..G;.5..H;.5..I;.5..J;.6..L;66..M;.6..N;.7..O;.7..P;.7..Q;>7..R;'8
..S;.8..T;+9..U;h9..W;.9..Y;.9..Z;.9..[;.9..\;.9..];.9..b;!:..c;K:..d;.:..e;.:..f;.:..g;.:..h;=;..i;.;..j;.;..m;.;..p;.<..q;#<..r;,<..s;2<..t;5<..u;L<..v;b<..w;}<..x;~<..y;.<..z;.<..{;.<..|;.<..};.=..
~;%=...;-=...;==...;N=...;.=...;.=...; >...;L>...;t>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>

C:\Users\user\AppData\Local\Programs\via\locales\sw.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	80058
Entropy (8bit):	5.378521333882305
Encrypted:	false
SSDEEP:	1536:FYjK2xEWpMJyF4OTcF4DigjeO4dHG5gQoaOnqtVaQIh1VhEOs+nc+oHw05:wxEtgF4OTcF4DigjPNDtVPe1VhI+nc+I

C:\Users\user\AppData\Local\Programs\via\locales\sw.pak	
MD5:	04842F2AF66FB58DF3E82F3EE0366DB6
SHA1:	CB1C5641E6B53C71EFEE2B996804B47DEA54EFBB
SHA-256:	7863CB871E8C97166F2AAC9DA58D63B8A165F3F390601A1AEC36406349185382
SHA-512:	EF4E2D2899C58292B7DDB4024B95C55EBF56396EA338A3A2933BF79A2CEAF3744DE739326994CF87D1B48D2E074FFAAFF1895ADBF8C30F52E09735D0C76A0BE 3
Malicious:	false

Preview:

............|..*..}..*..~..+.....+.....+.... +....&+....5+....F+....O+....d+....q+....w+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....+,....B,....I,....N,....U,....Z,
....a,....d,....e,....l,....x,.....,.....,.....,.....,.....,.....,..!..,..".,...:,...:.-...:(-...:;-...;j-...;.-...;.-...;.-...;.-...;.-...;.....;6....;@....;.....;.....;(/...;;/...;E/...;I/.. ;^/..#;e/..$;l/..%;./..&;./..(;./..);.0..*;(0
..+;40..,;>0..-;W0...;.0../;.0..0;`1..1;.1..2;g2..3;.2..4;.3..5;?3..6;N3..7;o3..8;.4..9;.4..:;.4..;;>5..<;o5..=;.5..>;76..@;.6..A;27..C;.7..D;.7..E;.7..F;.7..G;.7..H;.7..I;.8..J;.8..L;I8..M;
.8..N;.9..O;-9..P;@9..Q;d9..R;r:..S;.:..T;_;..U;.;..W;.;..Y;.;..Z;.;..[;.;..\;.;..];.<..b;[<..c;.<..d;.<..e;.<..f;.=..g;A=..h;.=..i;.=..j;6>..m;Y>..p;.>..r;.>..s;.>..t;.>..u;.>..v;.>..w;.>..x;.>..y;.>
..z;.>..{;!?..|;4?..};l?..~;s?...;|?...;.?...;.?...;.?...;;@...;s@...;.@...;.@...;.@...;.@...;.@...;.@...;.@...;.A...;.A...;.A...;.A...;%A...;)A...;-A

C:\Users\user\AppData\Local\Programs\via\locales\ta.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	195736
Entropy (8bit):	4.240058259742912
Encrypted:	false
SSDEEP:	1536:a7i5r1tD0DOTbej23CA+fp2E2k4ca6QVW0Yg1ortR6L+EZ5a5Au5KVn2nYhTF6c5:a7i5r1GDO2j236tRer
MD5:	2878E0F7E5E2B0B0BB5C0A4F7345515F
SHA1:	8D8832B8FBD7F94F14A540E07B548948D9FE31E4
SHA-256:	E242CCE909C4DEC25C81EAEC3E17C7261EDC5633F774D63A74CA22E545D19E59
SHA-512:	D15A481BDB68CC1CC7F46141D36B46F9804935F36E9898A2551F803239F55BA018F84D9488A4C3C5824CDA03ED582D1F6BB507BC978C000FD84677782E07CC14
Malicious:	false

Preview:

............|..*..}..*..~..+.....+.....+....$+....*+....9+....J+....S+....h+....u+....{+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....:,....z,.....,.....-....3-....Q-....f-....r-....y-....
|-....}-.....-.....-.....-..........=....................!....."......:./...:-/...:./...:./...;.0...;F1...;.1...;.1...;.1...;h2...;.2...;.2...;.3...;.4...;.4...;.5...;.5...;.5...;.5.. ;.6..#;)6..$;;6..%;p6..&;.6..(;c7..);.7..*;.7
..+;)8..,;D8..-;.8...;09../;.:..0;.;..1;.=..2;W>..3;.?..4;.@..5;.@..6;.@..7;6A..8;.B..9;.D..:;<E..;;.E..<;$F..=;.F..@;.H..C;.I..D;CI..E;qI..F;.I..G;.I..H;.I..I;.J..J;TJ..L;.J..M;XL..N;ZM..O;
.M..P;.N..Q;}N..R;.Q..S;DR..T;RS..U;RT..W;.T..Y;.T..Z;.T..[;.U..\;8U..];.U..b;vV..c;.V..d;.W..e;.X..f;.X..g;.Y..h;4Z..i;.[..j;.[..m;]\..p;.\..q;.\..r;.]..s;.]..t;']..u;g]..v;.]..w;.]..x;.]..y;.^..z;.^..
{;.^..|;.^..};i_..~;._...;._...;._...;._...;8a...;.a...;Nb...;.b...;.c...;.c...;.c...;(c...;0c...;3c...;=c...;@c...;Jc...;Mc...;bc...;fc...;xc...;zc

C:\Users\user\AppData\Local\Programs\via\locales\te.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	184081
Entropy (8bit):	4.4186069721788215
Encrypted:	false
SSDEEP:	3072:4i+BZuswrKJA7Hi9x6cH/VTCIAgbSqBdzEkXQtG5KLwD7x+mU/:GZVwrKJAWBH/V2IAgbSqBdzEkXQtGwLT
MD5:	D432CBEF00995B40C6F1D1AC28F48FC7
SHA1:	3B25E1514671F5488C27AA9921B463313151B035
SHA-256:	98ADC97B9CE5ADD5D8D7AD43FD74C50E760E17D1CA4AF7EFF81FB488963FCE0C
SHA-512:	744938779052543686DF0A68603D9E47AA90012EE3B64BF4E57FEAD3CABE6E4C7B8AE0620D728C77BBB2BD2C4FEF718FBCBBB54EA9AB32054D6BECCD6B0C6 BE8
Malicious:	false

Preview:

............|..+..}.#+..~..+....6+....;+....H+....N+....]+....n+....w+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,....9,....m,.....,.....,....$-....K-....r-.....-.....-.....-....
.-.....-.....-.....-..........&.....W....................!../.."../...:!/...:I/...:./...:./...;M0...;.0...;$1...;l1...;.1...;.2...;N2...;.2...;.2...;.3...;\4...;.4...;.5...;G5...;S5.. ;.5..#;.5..$;.5..%;.5..&;56..(;.6..
);G7..*;.7..+;.7..,;.7..-;38...;.8../;.9..0;.:..1;.<..2;<=..3;.>..4;.>..5;.?..6;C?..7;.?..8;UA..9;VC..:;.C..;;!D..<;sD..=;.D..>;(F..@;pG..A;~H..C;.I..D;.I..E;.I..F;.J..G;2J..H;nJ..I;.J..J;.J
..L;VK..M;.L..N;.M..O;.M..P;.M..Q;^N..R;.P..S;.Q..T;iR..U;;S..W;.S..Y;.S..Z;.S..[;.S..\;3T..];.T..b;pU..c;.U..d;.V..e;AW..f;.W..g;.W..h;.X..i;.Y..j;`Z..m;.Z..p;.[..q;$[..r;B[..s;K[
..t;c[..u;.[..v;.[..w;G\..x;H\..y;.\..z;.\..{;.\..|;.]..};.]..~;.]...;.^...;.^...;V^...;._...;+`...;.`...;.`...;Ja...;.a...;.a...;.a...;.a...;.a...;.a...;.a...;.a...;.a...;.b...;.b

C:\Users\user\AppData\Local\Programs\via\locales\th.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	159993
Entropy (8bit):	4.515421369825943
Encrypted:	false
SSDEEP:	3072:KilC40CJFkSCkIOBVVmMRD+Puv3bUGw1pSd9zlv7QbAdhl0qZtJClRR/v0:KdCJFkSCkIOBV5qPuv3bUGw1pSd9zlU4
MD5:	905F032DB6E1D6C4C93E35A875532190
SHA1:	583EE5F4651D4BF6C6C827796CB087C9AD7F5EC4
SHA-256:	23762FB4F440544E02E58512A917DD02D8859323722645836 80AC870558473A6
SHA-512:	5BFAA0677E9CA376D62642391E7A9B7D0FA1E228DFAFF0CD29A7E2A6D70C784FF72E846AA7C81422A846A5B22F45274840600A65D50621794F28AD797FBEA19E
Malicious:	false

C:\Users\user\AppData\Local\Programs\via\locales\th.pak

Preview:


```
............|..*..}..*..~..*.....*.....*.....*.....+.....+.....+....2+....?+....E+....T+....Z+....l+....t+....y+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....Z,....~,.....,.....,.....,.....,.....,.....,.....-
....)-....5-....G-....z-.....-.....-.....-..!..-.."..-...:.....:#....:f....:.....;.....;z/...;./...;./...;./...;O0...;.0...;.0...;.0...;u1...;.1...;U2...;.2...;.2...;.2.. ;.3..#; 3..$;/3..%;V3..&;t3..(;.4..);\4..*;.4..+;.4..,;.4..-
;.4...;P5../;N6..0;s7..1;.8..2;.9..3;`;..4;.;..5;.;..6;.;..7;(<..8;s=..:;.?..;;.?..<;.?..=;N@..>;.A..@;.B..A;,D..C;NE..D;cE..E;.E..F;.E..G;.E..H;.E..I;.F..J;7F..L;.F..M;xG..N;=H..O;bH..P;
.H..Q;.H..R;SK..S;QL..T;!M..U;.M..W;.M..Y;.M..Z;.N..[;/N..\;JN..];.N..b;.O..c;kO..d;YP..e;.P..f;.P..g;.P..h;.Q..i;\R..j;.S..m;MS..p;.S..r;.S..s;.S..t;.S..u;.T..v;XT..w;yT..x;zT..y;
.T..z;.T..{;.T..|;.T..};kU..~;.U...;.U...;.U...;.U...;.V...;qW...;.W...;`X...;.X...;.X...;.X...;.X...;.X...;.X...;.X...;.X...;.X...;.Y...;.Y...;.Y...; Y...;"Y...;+Y...;@Y
```


C:\Users\user\AppData\Local\Programs\via\locales\tr.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	82934
Entropy (8bit):	5.6362117684923
Encrypted:	false
SSDEEP:	1536:PQtPeptagXAOv+yLPhRNH2Hjn4hnMeuCxWd57YBSJ81tZRhEBD8GKUnjubI3Fr:PQt2ptagXAOv+yLPNH2HWnMedBw81PrI
MD5:	21B06573A05893036A92F47E6CB965BF
SHA1:	3D9DAC87C966747A967FE9C4EEF25C279D40B027
SHA-256:	16FD586BE5F204F203150531D2F8423ED9C3C185EE7702F1D775CA15B67BDE38
SHA-512:	94E5881075422F13CCC215D4CEF9FE3A2559A11763E6F953A479478D98B316E4E00C431F9442521FFEFD54E3F92822D66B6FB7DA74ED0C436B3C99290092E192
Malicious:	false

Preview:


```
............|..+..}..+..~..+....$+....)+....6+....<+....K+....\+....e+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,....3,....I,....c,....{,.....,.....,.....,.....,....
.,.....,.....,.....,.....,.....,.....,.....,.....,..!..-.."..-...:$-...:<-...:n-...:.-...;.-...;.-...;.....;#....;(....;_....;z....;.....;.....;./...;b/...;./...;./...;./...;./.. ;./..#;./..$;./..%;./..&;.0..(;O0..);u0..*;.0..+;.0..,;.0..-
;.0...;.0../;X1..0;.1..2;<2..3;.2..4;.2..5;.2..6;.3..7;.3..8;.3..9;l4..:;.4..;;.4..<;.4..=;.5..>;.5..@;.6..A;.6..C;.7..D;.7..E;.7..F;.7..G;+7..H;;7..I;L7..J;c7..L;.7..M;.8..N;{8..O;.8..P;.8..Q;.8
..R;.9..S;h:..T;.:..U;.;..W;';..Y;-;..Z;>;..[;G;..\;U;..];|;..b;.;..c;.;..d;L<..e;q<..f;.<..g;.<..h;.=..i;h=..j;.=..m;.=..p;.>..q;.>..r;.>..s;.>..t;.>..u;2>..v;G>..w;f>..x;g>..y;w>..z;z>..{;.>..|;.>..
};.>..~;.?...;.?...;.?...;'?...;.?...;.?...;&@...;S@...;y@...;.@...;.@...;.@...;.@...;.@...;.@...;.@...;.@...;.@...;.@...;.@
```


C:\Users\user\AppData\Local\Programs\via\locales\uk.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	137010
Entropy (8bit):	5.055989661678431
Encrypted:	false
SSDEEP:	3072:pDYGvB3IjpPkSzLwRPu0VZCDLNiXMlQUCqJ7MVUMTEb4UsJo:lvB3Ijp1tLNiXMjCqJCq
MD5:	CD0E720F7685CEC9DE1C7106A17D369D
SHA1:	7CA1FB0EABD13BB3A5ADA0084F1CA6ADC76189D9
SHA-256:	294A0ACE6F5BE8F6EB9612DA3C6A96D7FE28B37055CCB50734B6939E267A0470
SHA-512:	E75B3117B3A57DBB8EAAA35AC97A15A9A4131094BA73B0D953E7D9990406E9A05B0154F51A737C9C3A51890BC4DC5D4567E7A42D38F24BFB6902FC0467D66C7 2
Malicious:	false

Preview:


```
............|..+..}..+..~..+....$+....)+....6+....<+....K+....\+....e+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....&,....P,....{,.....,.....,.....,.....,.....,.....-.....-
.....-.....-....3-....=-....O-....c-.....-.....-.....-..!..-.."..-...:.-...:.....:h....:.....;.....;m/...;./...;./...;./...;./...;.0...;=0...;[0...;.1...;.1...;.2...;G2...;W2...;e2.. ;.2..#;.2..$;.2..%;.2..&;.2..(;e3..);.3..*;.3
..+;.3..,;.3..-;.4...;|4../;!5..0;.5..1;.6..2;~7..3;g8..4;.8..5;.8..6;.9..7;N9..8;):..:;h;..;;.;..<;.<..>;g<..A;9=..C;.=..D;.>..E;.>..F;0>..G;K>..H;w>..I;.>..J;.>..L;.?..M;.?..N;.A..O;.A..P;
.A..Q;.A..R;.F..S;.H..T;.I..U;.I..W;.J..Y;#J..Z;FJ..[;_J..\;|J..];.J..b;FK..c;.K..d;-L..e;TL..f;.L..g;.L..h;.M..i;.N..j;wN..m;.N..p;*O..r;@O..s;LO..t;RO..u;.O..v;.O..w;.O..x;.O..y;.O..z;.P..
{;JP..|;vP..};.P..~;.P...;.P...;.Q...;%Q...;.Q...;lR...;.R...;.S...;6S...;FS...;JS...;US...;]S...;`S...;jS...;mS...;wS...;zS...;.S...;.S...;.S...;.S...;.S...;.S
```


C:\Users\user\AppData\Local\Programs\via\locales\vi.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	96974
Entropy (8bit):	5.818608245212573
Encrypted:	false
SSDEEP:	1536:XTf8OZG5ICMm2KAPnijSPiz+sJ6m9+e8Mv2nclg4m9WbICkoqC+bkW8TWilnd0CE:Xj8wm2KAPni+Piz+sJ6m92Mv2LT9WbtM
MD5:	5BACF8E262496C2FABF14D30FA1BAB2E
SHA1:	8027235A5B8E6D91A6D8F4C6AA3F8F641B8BB62D
SHA-256:	BD0B9D7C10F2A50B0B98791794145841636D2C5B8D36A4854BEAC2E64EBBD469
SHA-512:	98F129286C434C33608D9033FB114C6518514C5C4DBFEC320A744AAA136BB1F9B3640C38321619491C92EE8E381CC3B47769B904EA6A77123F7F5A56A92F07A2
Malicious:	false

Preview:


```
............|..*..}..*..~..*.....+.....+.....+.....+....-+....>+....G+....\+....i+....o+....~+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,....F,....e,....n,....w,.....,.....,.....,....
.,.....,.....,.....,.....,.....,.....,.....-.....-..!..-.."..-...:8-...:E-...:t-...:.-...;.-...;.-...;.....; ....;....;u....;.....;.....;.....;!/...;./...;./...;./...;./...;./.. ;.0..#;.0..$;"0..%;-0..&;70..(;.0..);.0..*;.0..+;.0..,;.0..-
;.1...;W1../;.1..0;d2..1;.3..2;.3..3;%4..4;54..5;i4..6;y4..7;.4..8;A5..9;16..:;U6..;;.6..<;.6..=;.6..>;.7..@;(8..A;.8..C;A9..D;J9..E;U9..F;_9..G;s9..H;.9..I;.9..J;.9..L;.9..M;s:..N;.:..
O;.:..P;.;..Q;';..R;]<..S;.<..T;o=..U;.=..W;.=..Y;.=..Z;.=..[;.=..\;.>..];3>..b;.>..c;.>..d;.?..e;??..f;Z?..g;.?..h;.@..i;p@..j;.@..m;.@..p;)A..q;4A..r;=A..s;CA..t;GA..u;aA..v;.A..
w;.A..x;.A..y;.A..z;.A..{;.A..|;.A..};IB..~;aB...;nB...;}B...;.B...;.C...;iC...;.C...;.C...;.D...;.D...;.D...;'D...;1D...;4D...;>D...;AD...;KD...;ND...;\D...;`D
```


C:\Users\user\AppData\Local\Programs\via\locales\zh-CN.pak

Process:	C:\Users\user\Desktop\via-1.3.1-win.exe

C:\Users\user\AppData\Local\Programs\via\locales\zh-CN.pak	
File Type:	data
Category:	dropped
Size (bytes):	72657
Entropy (8bit):	6.7081756756151485
Encrypted:	false
SSDEEP:	1536:+ee7f6LcBJO/ggdzemjWPJkWhc9WRlsWEu:feX3O/ggdzemKakUWlku
MD5:	DEE4A1A5BAF9B01303F09945DDACD1D9
SHA1:	58EFEF6EC440EAB597197CDC1DF959B7B9E4EC24
SHA-256:	694C61983F5DF925CB9AE5573AB24A430207C227092270BA1581679E774A1921
SHA-512:	DD8BBD0712CA1C53644AEA1E446631C21C5591552AFB283BF7BF27F35B8343EBCE7A7C1571EBB188F3BEB2882B3175734F66C5E7D1D5A75C2815B4488B04C71 0
Malicious:	false
Preview:	............|..*..}..*..~..*.....*.....*.....*.....*.....*.....+.....+....!+.....+....4+....F+....N+....V+....a+....i+....x+....}+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,.....,.....,.... .,....!,....',....-,....9,....M,....V,....\,..!.h,..".k,...:,...:,...:,...:,...;,...;.-...;%-...;:-...;@-...;m-...;.-...;.-...;.-...;.....;?....;n....;{....;.....;.... ;....#;....$;....%;....&;....(;./..);H/..*;W/..+;c/..,;i/..-;x/...; ./../;.0..0;.0..1;.1..2;.1..3;I2..4;X2..5;{2..6;.2..7;.2..8;&3..9;.3..:;.3..;;)4..<;O4..=;x4..>;.5..A;.5..C;.6..D;"6..E;+6..F;16..G;:6..H;I6..I;Z6..J;r6..L;.6..M;.6..N;v7..O;.7..P;.7..Q;.7.. R;r8..S;.8..T;>9..U;t9..W;.9..Y;.9..Z;.9..[;.9..\;.9..];.9..b;2:..c;P:..d;.:..e;.:..f;.:..g; ;..h;.;..i;.;..j;.<..m;L<..p;v<..q;|<..r;.<..s;.<..t;.<..u;.<..v;.<..w;.<..x;.<..y;.<..z;.<..{; =..|;4=..}; j=..~;v=...;|=...;.=...;.=...;.=...;2>...;c>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.>...;.?...;.?...;.?...;.?...;5?

C:\Users\user\AppData\Local\Programs\via\locales\zh-TW.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	72935
Entropy (8bit):	6.706836138074188
Encrypted:	false
SSDEEP:	1536:ZZDSxqJ1u9htEjnuRtedHG/ape3mPzJ80aHYRhbfSxzVnBAJ5HV3XiPnhb5mxgTv:ZAxu8LYnuRtedHVX180fmoJ5H9XiPhbB
MD5:	B3A5AA832E2572F6B932D3444B9D7E1D
SHA1:	10843DDAB1F71C4AE5810D5FDCDD51F547648C43
SHA-256:	38F6A0FEA3F2EB4147FEF2008A5B7757AC8F44BD704B194E09CB2DD30D6A90EE
SHA-512:	585191A0267B42F18615F28AFB2F87555843F637124E9F3B6449735B7B1729A4C078AF2152AC0A313F21C1621C0229D9263F9B6DE8633A418E3A500293EA832E
Malicious:	false
Preview:	............|..*..}..*..~..*.....*.....*.....*.....*.....*.....+.....+....++....8+....>+....M+....S+....e+....m+....r+....z+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....+.....,.....,.....,.....,.....,.... .,....(,.....,....4,....@,....T,....],....c,..!.o,..".r,...:,...:,...:,...:,...;,...;)-...;>-...;Y-...;_-...;.-...;.-...;.-...;.-...;.....;[....;.....;.....;.....;.... ;....#;....$;....%;....&;....(;D/..);s/..*;./..+;./..,;./..-;./...; ./../;S0..0;.0..1;A1..2;.1..3;M2..4;\2..5;.2..6;.2..7;.2..8;+3..9;.3..:;.3..;;/4..<;X4..=;.4..>;.5..@;.5..A;.5..C;l6..D;~6..E;.6..F;.6..G;.6..H;.6..I;.6..J;.6..L;.7..M;q7..N;.7..O;.7..P;.7.. Q;.8..R;.8..S;O9..T;.9..U;.9..W;.9..Y;.9..Z;.:..[;.:..\;.:..];>:..b;.:..c;.:..d;.;..e; ;..f;/;..g;Z;..h;.;..i;.<..j;C<..m;m<..p;.<..q;.<..r;.<..s;.<..t;.<..u;.<..v;.<..w;.<..x;.<..y;.=..z;.=..{;F=..|; Z=..};.=..~;.=...;.=...;.=...;.=...;.>...;a>...;.>...;.>...;.>...;.>...;.>...;.>...;.?...;.?...;.?...;.?...; ?...;#?...;/?...;3?...;<?...;@?

C:\Users\user\AppData\Local\Programs\via\natives_blob.bin	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	82118
Entropy (8bit):	5.034992186435272
Encrypted:	false
SSDEEP:	1536:+bz4Oif2sMnL8gDpKD0rrr/4or06mGsY3csV3iEBSsU0fHBvJ4YfD3z5Q29ei7gy:+bz4Oif2sMaEBSJ0fHBvOYbj5heikwVJ
MD5:	1582FFE1B8CB37438BC22EDEE6CD0A90
SHA1:	01AF249F33B2E5FFBA18BA8F7CD76F2EE0E5F425
SHA-256:	02586EEAF4CE40D1B34310D885E34FB63E8E9F155FCEDBD796536735907CBE80
SHA-512:	8C66BA4EF15FEA573C29F0F6977E290B8FD72F4C8833F31A9B0EF4285F5493E9B27DAF3A02C352ED12EADCE36CDA933D9D97576BFA4DCBBCC04294E73AD9E FC
Malicious:	false
Preview:	@CommonOperationsU..(function(global, binding, v8) {.'use strict';.const _queue = v8.createPrivateSymbol('[[queue]]');.const _queueTotalSize = v8.createPrivate Symbol('[[queueTotalSize]]');.const _isSettled = v8.createPrivateSymbol('isSettled');.const Boolean = global.Boolean;.const Number = global.Number;.const Number _isFinite = Number.isFinite;.const Number_isNaN = Number.isNaN;.const RangeError = global.RangeError;.const TypeError = global.TypeError;.const TypeError_protot ype = TypeError.prototype;.const hasOwnProperty = v8.uncurryThis(global.Object.hasOwnProperty);.const getPrototypeOf = global.Object.getPrototypeOf.bind(global. Object);.const getOwnPropertyDescriptor =.global.Object.getOwnPropertyDescriptor.bind(global.Object);.const thenPromise = v8.uncurryThis(Promise.prototype.then) ;.const JSON_parse = global.JSON.parse.bind(global.JSON);.const JSON_stringify = global.JSON.stringify.bind(global.JSON);.function hasOwnPropertyNoThrow(x, prop erty) {.return Boolean(x) && hasOwnPrope

C:\Users\user\AppData\Local\Programs\via\resources.pak	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	8657690
Entropy (8bit):	6.565783719566008
Encrypted:	false
SSDEEP:	98304:q7DB/Q9d5h3I2qd9VUtC1hhNm589CG+8bytTwU:GDB/yd5h3ydxhfw1aWtX

C:\Users\user\AppData\Local\Programs\via\resources.pak	
MD5:	ECE1281ABFE1F39AECBD5250D5252403
SHA1:	9F995DAEC49CDB2A3F60C93B3DBF53C6CA0941E4
SHA-256:	64725EEE7BE0C64D7D034E77EE0B4A229D59A0865539C3E70CC7A534A89B5182
SHA-512:	CD78A0125BB77C9DCEA4616544117789BC2D5C75D48123AC50B1AACCFD14AB43955850C155B4DD875DC34FCA813E9CC7030EDA2EE7CC71E418F384F19686FB4
Malicious:	false
Preview:	.....B10...C1.{..:C1...;C>...<C....=CO...>C.`..?CFd..@Cwi..AC.r..BC.t..CC.u..DC.y..EC&|..FCd...GC.(..HCa1..IC.2...JC.3..KC.4..LC.9..MCq;..NC.@..OC.E..PC.Z..QC.o..RC.t..SC.u..TCb}..UC]...VC....`Cml..aC.q..bC.t..cC,v..dC.}..eC...fC....gC....hC...iC...jCT...kCt...lC,+..mC.M..nC.O..oCLQ..pC.S..qC.Y..rCWa..sCzv..tChx..uC....vCQ...wC....xC...yC....zC....{C...|C}...}C....~C\....C.....C.....Cl....C;....C.....C.....C.....O.....O.....O.....O.....Ob....Op....Ot....O.....O.#...O.%...OX'...O}/...O.3...O{6...O.?...O.^...O.`...OZf...Ozg...O.h...O.j...O.o...O.w...Ojz...O7....O....O....O....O....O....Ou....O.....O....FP....GPx....ae....a.<...a>=...aJl...aGm...a.o...a.p...akr...a.s...a\u...aTv..:a/x...cu.....c.....c....cC....c....c....c....c.....c(....c(....c.....c.....cL....c.....c.....c.....c'....c.....c.....c.....cJ....c.....c.....c.....c$"...co$...c.-...c./...c.3...c.@...c.C...c.L...c.N...c{....c_....c....c.....c.....c^....c.....c.....cg....c.....c.....c.6...c.6...c)9...c.;

C:\Users\user\AppData\Local\Programs\via\resources\app-update.yml	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	C++ source, ASCII text
Category:	dropped
Size (bytes):	119
Entropy (8bit):	4.381045685491536
Encrypted:	false
SSDEEP:	3:8trthvQOxrwhFPEP6iWNZRBDEK9MsAfaXSWQnAhAB48:2PDrSg65B9WfaiWQn5
MD5:	276BED0C03C960939367ACBAA5F5200E
SHA1:	C8DF487D68EFAFAFC994D29A651F12F70827D155
SHA-256:	AB190A11E84475D0EA8CE35C4422E862F2764DF9F190BC1B3300C14921E8B226
SHA-512:	32CEAE5DE2D6165543507F0AF714D7389C8C210858CD3B15D1A62870D47160DBDF87890DA39AF35EF923470D125CCC589C35C84AA7621FA340095F88011AF8B
Malicious:	false
Preview:	owner: the-via.repo: releases.provider: github.publishAutoUpdate: true.private: false.updaterCacheDirName: via-updater.

C:\Users\user\AppData\Local\Programs\via\resources\app.asar	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	156562733
Entropy (8bit):	5.78891096301091
Encrypted:	false
SSDEEP:	786432:AOzaYHvGLXO7pG166xBe/rp7TEjT2ET2XT2LT2OT2rhwNFgvQIGfmkW:sYHvMO7pG166xBe/rx
MD5:	55001FD547AACB13EC23183DE8916A3E
SHA1:	48A68946F52304FB53D4AF6A23BB6D5758DE6F8E
SHA-256:	C963E8C99DEE8452E2FC431877F71C675960A0817B6DAE089BB716A363B52AF2
SHA-512:	C7C90F6DB2717A900A01037747B29952FED537E58DAD05F9735BDC986EF2179915FF9880398244AB3278B508FD0BF146EDF5DC179D61D16DFB466C19809AD93E
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Predator, Description: Yara detected Predator, Source: C:\Users\user\AppData\Local\Programs\via\resources\app.asar, Author: Joe Security
Preview:	.....{"files":{"package.json":{"size":3560,"offset":"0"},"app":{"files":{"app.html":{"size":1248,"offset":"3560"},"main.prod.js":{"size":237763,"offset":"4808"},"main.prod.js.map":{"size":280637,"offset":"242571"},"dist":{"files":{"084f7589f4bfa02922a3fbcc896f0887.woff2":{"size":14171,"offset":"523208"},"088a34f78f530102fd9661173b4a4f26.eot":{"size":131930,"offset":"537379"},"1058c860eff7cd398786334414e6a5ea.ttf":{"size":2169800,"offset":"669309"},"15776eec451ff4c88330cc66edd9e1e4.woff":{"size":19248,"offset":"2839109"},"17ea4760cdf09ade45a20bce5f2933a9.woff":{"size":18008,"offset":"2858357"},"18dd4f87fffded28ff1bb467f5b0709f.woff":{"size":18584,"offset":"2876365"},"194f8b761e47d7f53e3ac96918f7eaa7.woff2":{"size":14491,"offset":"2894949"},"19e60b83eaed98dd4409aa4ec4880f66.woff2":{"size":14003,"offset":"2909440"},"1a0fda4533853faab45697ee60d0f9fe.woff2":{"size":14548,"offset":"2923443"},"1a4bcb3ec9c508d478d4dbf6b56f6208.woff2":{"size":15764,"offset":"2937991"},"273dc9bf9778fd

C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107520
Entropy (8bit):	6.442687067441468
Encrypted:	false
SSDEEP:	
MD5:	792B92C8AD13C46F27C7CED0810694DF
SHA1:	D8D449B92DE20A57DF722DF46435BA4553ECC802
SHA-256:	9B1FBF0C11C520AE714AF8AA9AF12CFD48503EEDECD7398D8992EE94D1B4DC37
SHA-512:	6C247254DC18ED81213A978CCE2E321D6692848C64307097D2C43432A42F4F4F6D3CF22FB92610DFA8B7B16A5F1D94E9017CF64F88F2D08E79C0FE71A9121E40
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	
Joe Sandbox View:	• Filename: eTrader-0.1.0.exe, Detection: malicious, Browse • Filename: eTrader-0.1.0.exe, Detection: malicious, Browse • Filename: w0Ku4mr4HN.exe, Detection: malicious, Browse • Filename: w0Ku4mr4HN.exe, Detection: malicious, Browse • Filename: , Detection: malicious, Browse • Filename: elior-1.13.4.exe, Detection: malicious, Browse
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\Programs\via\snapshot_blob.bin	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	280424
Entropy (8bit):	4.674571575845
Encrypted:	false
SSDEEP:	
MD5:	C064BE25C39B7B862F284FAF9916E244
SHA1:	C4C17C1BC40A17BC319FEAD8C982E7A59233FC82
SHA-256:	4F0195B0B6B5BE146396C38450C89BE519AEF9244887991DB4955E50E167EB59
SHA-512:	DA7B7E781C61957FDB174960B082786373623BB2711D079DE48A317A086676E3CA9E7071BFA6464ADC318844172C124E59095AA61FB1423B9399E9938A33EDC9
Malicious:	false
Preview:	.....2....c7.8.279.23-electron.0.....0...(S.....>...Q.....`.....`.....`.....`....5...`.....`..... ....m.`....$...D..X!q...X!5...X!5.D. ..M.`....$...D..X!a...X!9...X!9.D. ..`....$...D..X!q...X!=...X!=.D. ....`....$...D..X!q...X!A...X!A.D. ..a.`....D...D..X!e...X!E...X!E.D. ....`....$...D..X!q...X!I...X!I.D. ..A.`....$...D..X!q...X!M. ..X!M.D. ..`....$...D..X!q...X!Q...X!Q.D. ..`....$...D..X!q...X!U...X!U.D. ....`....$...D..X!i...X!Y...X!Y.D. ..`....$...D..X!q...X!]...X!].D.(Ja....!.....@.....F^`.....V`.....`.....(J a....1.....@.....F^`.....A.`.....@...IDa.....D`.....D`.....D`.....`.....D]....D`.....V`.....WIa.....V`.....WIa.....WIa.....WIa..... .....V`.....WIa.....WIa.....WIa.....V`.....WIa.....WIa.....

C:\Users\user\AppData\Local\Programs\via\swiftshader\libEGL.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	341504
Entropy (8bit):	6.185245468840032
Encrypted:	false
SSDEEP:	
MD5:	948D32BC09B77C82B2D6E9D1B84B0805
SHA1:	F38EEF56E29B16E73D49D21510A7575A716BCDD3
SHA-256:	EC8706A9EE63CD6B497C8220ABADA9988A8A86844FF924C1F413697DCBBEB867
SHA-512:	BD77029A7F02FF6511DB7342DC4501C266C3F58FE6A25EBDF56A3F7F041FC19F867E56C723CB74E82F7AE6B97A873ED1895F36D7F66A39CECEADB8442DDF07 7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...,..]....." .....d.....D.....`..... .....v.....{..P..... ...>.....u.....F..(.....text....b.....d..... ..`.rdata..TQ.....R...h..... @..@.data....;.....$.....@....pdata...>... ...@.....@..@.00cfg.....`.....@..@.tls.....p..... .....@....rsrc....."".....@..@.reloc..... .....(.....@..B..... .....

C:\Users\user\AppData\Local\Programs\via\swiftshader\libGLESv2.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3841536
Entropy (8bit):	6.238064006123621
Encrypted:	false
SSDEEP:	
MD5:	FA296B797F2F10EFA41C168652BBE8D9
SHA1:	A4CC567582F80F8E328ECB31A37F9CE7159BA266
SHA-256:	2564E16FD6A5DCDC6FAB5C26237DAD23BA3D839AA5361A9DE7C7EBA4C88E2247
SHA-512:	AC156316211C52012C14A71AFDD5160AE353A6E9A9AC38E9976B7A959C46864A0D1FC0C17B7815BC89B5E9B37AB1E3EBA1A3EE0B80F490E2AB42EF7BD42FDC 42
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Programs\via\swiftshader\libGLESv2.dll	
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...,..]....." .....4.....1.....?.....`..... .....Z8.. ..u{8.d....?.....P>.<#.....?..:...X8.....x 8.(....P7.....`.8.....text...V.4.....4..... ..`.rdata...P....4..R....4... .....@..@.data....-... 9..4....9.....@....pdata..<#...P>..$...69.....@..@.00cfg.....?.....Z:.....@..@.tls....%....?.....\:.....@....rsrc.....?.....^:..... @..@.reloc...:....?..<...b:.....@..B..... .....

C:\Users\user\AppData\Local\Programs\via\v8_context_snapshot.bin	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	data
Category:	dropped
Size (bytes):	701096
Entropy (8bit):	4.977074548202187
Encrypted:	false
SSDEEP:	
MD5:	ADE12ED60B340F474E242F66BA423711
SHA1:	4D800CD71872E76E08A5A5650FF0169EB16F8EF6
SHA-256:	25B3A8326201F6940611C49EABECAFF1648D31C27FF38DD192015B23E7DC75E0
SHA-512:	2CB2AF6E0F873A36ABA90307FBA0B56A039F1EE29F317C70C5FC41634B19F6C0A807AA9293CBF7A83F470637921DDC96F79B4273300A61259447FCE0624A097E
Malicious:	false
Preview:	.....\.....7.8.279.23-electron.0.....P...H}...q..".....h#...Q.....`.....`.....`....<...`.....`....5...`.....`..... ....m.`....$...D..X! q...X!5...X!5.D. ..M.`....$...D..X!a...X!9...X!9.D. ..`....$...D..X!q...X!=...X!=.D. ....`....$...D..X!q...X!A...X!A.D. ..a.`....D...D..X!e...X!E...X!E.D. ....`....$...D..X!q...X!I...X!I.D. ..A.`....$ ...D..X!q...X!M...X!M.D. ..`....$...D..X!q...X!Q...X!Q.D. ..`....$...D..X!q...X!U...X!U.D. ....`....$...D..X!i...X!Y...X!Y.D. ..`....$...D..X!q...X!]...X!].D.(Ja....!.....@.....F^`.....V`.... ....`.....(Ja....1.....@.....F^`.....A.`.....@...IDa.....D`.....D`.....D`.....`.....D]....D`.....V`.....Wla.....V`.....Wla.....Wla..... ...Wla.....V`.....Wla.....Wla.....Wla.....V`.....Wla.....Wla

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\SpiderBanner.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9216
Entropy (8bit):	5.5347224014600345
Encrypted:	false
SSDEEP:	
MD5:	17309E33B596BA3A5693B4D3E85CF8D7
SHA1:	7D361836CF53DF42021C7F2B148AEC9458818C01
SHA-256:	996A259E53CA18B89EC36D038C40148957C978C0FD600A268497D4C92F882A93
SHA-512:	1ABAC3CE4F2D5E4A635162E16CF9125E059BA1539F70086C2D71CD00D41A6E2A54D468E6F37792E55A822D7082FB388B8DFECC79B59226BBB047B7D28D44D25 8
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.../../../..Wy./../../...../..Wi./..Wx./..W~./..W{./..Rich./.....P E..L...T{mW.....!.....p!.....0.....p.....@.....5..o...l1..P....P.....`.....0.....te xt..... ..`.rdata.....0.....@..@.data.....@.....@....rsrc.....P.....@..@.reloc..d...`..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\StdUtils.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	102400
Entropy (8bit):	6.729923587623207
Encrypted:	false
SSDEEP:	
MD5:	C6A6E03F77C313B267498515488C5740
SHA1:	3D49FC2784B9450962ED6B82B46E9C3C957D7C15
SHA-256:	B72E9013A6204E9F01076DC38DABBF30870D44DFC66962ADBF73619D4331601E
SHA-512:	9870C5879F7B72836805088079AD5BBAFCB59FC3D9127F2160D4EC3D6E88D3CC8EBE5A9F5D20A4720FE6407C1336EF10F33B2B9621BC587E930D4CBACF33780
Malicious:	false
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.[.C...CRich...C.....PE..L...I..[.....!.....*...b.....@.....+....@.....}..d....t.....X..... .....@.....text....).....*..... ..`.rdata..TC...@...D.....@..@.data...l.....r.....@....rsrc...X.....x.....@..@.reloc..j..... .....~.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.890541747176257
Encrypted:	false
SSDEEP:	
MD5:	75ED96254FBF894E42058062B4B4F0D1
SHA1:	996503F1383B49021EB3427BC28D13B5BBD11977
SHA-256:	A632D74332B3F08F834C732A103DAFEB09A540823A2217CA7F49159755E8F1D7
SHA-512:	58174896DB81D481947B8745DAFE3A02C150F3938BB4543256E8CCE1145154E016D481DF9FE68DAC6D48407C62CBE20753320EBD5FE5E84806D07CE78E0EB0C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....oZ.....!..... .....)......0.....`.....@.....2.....0..P.....P.....0..X. .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...x....@.....(.....@....reloc..~....P.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\WinShell.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	3.3907428713435226
Encrypted:	false
SSDEEP:	
MD5:	1CC7C37B7E0C8CD8BF04B6CC283E1E56
SHA1:	0B9519763BE6625BD5ABCE175DCC59C96D100D4C
SHA-256:	9BE85B986EA66A6997DDE658ABE82B3147ED2A1A3DCB784BB5176F41D22815A6
SHA-512:	7ACF7F8E68AA6066B59CA9F2AE2E67997E6B347BC08EB788D2A119B3295C844B5B9606757168E8D2FBD61C2CDA367BF80E9E48C9A52C28D5A7A00464BFD2048 F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[.....[....[....[...Rich.....PE..L.....1T.....''!..... .....0.....<..... ..4.....text...B..... ..`.reloc..L.... .. ..@..B.....

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	7-zip archive data, version 0.4
Category:	dropped
Size (bytes):	71465100
Entropy (8bit):	**7.9999961187766155**
Encrypted:	**true**
SSDEEP:	
MD5:	1999F5E65FB8592F93802EC03B1F9566
SHA1:	CBB4A5F97C07248140666D807A07253FE6473DAD
SHA-256:	DD8A65F812689580A67D2836C96D4B585D8539A3ACD31CB9C8E69BC3D9FC2045
SHA-512:	4F9F7C6C986C4693DD7978CE800D0C12030B8E9FBCC8A72930EA7D7603A9B31C30B816341C07FD58D028920B4E0F41F8D7C2B1F03749A2DF96DF0F1901E192A
Malicious:	false
Preview:	7z..'....B.,GxB.....%.....9..]...6....za.....@.8..qh...j..\Ed. b.E.....j...".4\...\..:H0...28m.....D.K..n..}.@.;....''..kCp.....Rx..k.....v.E~.WI=...n...*..5.....-C..4...m.{}.....C... .S._...e.3.\e3^y=....0..%...MA...>.d.w...F....9....c.v...ir@9..q..(.....#}.-...3.....~.d<U.....<..S..L..[...s..}...YXh/...z.O..7Z%h..'./K.....@.....{B.....1.c....b...K.hL..cB.. .^.Z...%.|... (<.j...Q.K<...].\0Uy&-.K.,n?..../.8..;.E....q.;.....?x..s.o._..2g....(..h!....._D..I.&..4!@.ekf.5E.i....R$RO:rP...2.c!?.....D?..-h.cR.s.3...y..4.`.UT..#h..#.p.46![....8.FYS.q_.z...._.O.. z.F..',p...n>F.Pw`....tB3P..'.QgWm.=...../Jx)....-P.\.....H..f...0.;...=.....V..(.T.P....#r...Gp.....&.&.3.T.S..o..Y.^..^...._...4?.x.aW..0J$0W..._..g.Xu...DZ^&...Y.....m.j.....x :FmK2.....(..L...t.\Z8?5..4.(..[..|.T{6...f.%.vP.H-\.6.,...:...7.% r.....FI.9M|....7}5.#.#.....&.j...9.....h...S]..}.....K_.j..(.(.w..B*<R...e...,.Z.?'..&.2f.^.....

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.703695912299512
Encrypted:	false
SSDEEP:	
MD5:	F0438A894F3A7E01A4AAE8D1B5DD0289

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	
SHA1:	B058E3FCFB7B550041DA16BF10D8837024C38BF6
SHA-256:	30C6C3DD3CC7FCEA6E6081CE821ADC7B2888542DAE30BF00E881C0A105EB4D11
SHA-512:	F91FCEA19CBDDF8086AFFCB63FE599DC2B36351FC81AC144F58A80A524043DDEAA3943F36C86EBAE45DD82E8FAF622EA7B7C9B776E74C54B93DF2963CFE66CC7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.I...I...I...n}f.L...I...P...@..K...@..H...@..H...RichI..... ...PE..L...\..N.....!..... ....`.....#..... ..<....@.....P..|..... ..d..... ..text..... ..`.rdata..... .....@..@.data... ....0.....@....rsrc.....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsis7z.dll	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	434176
Entropy (8bit):	6.584811966667578
Encrypted:	false
SSDEEP:	
MD5:	80E44CE4895304C6A3A831310FBF8CD0
SHA1:	36BD49AE21C460BE5753A904B4501F1ABCA53508
SHA-256:	B393F05E8FF919EF071181050E1873C9A776E1A0AE8329AEFFF7007D0CADF592
SHA-512:	C8BA7B1F9113EAD23E993E74A48C4427AE3562C1F6D9910B2BBE6806C9107CF7D94BC7D204613E4743D0CD869E00DAFD4FB54AAD1E8ADB69C553F3B9E5BC6DF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.6a..X2..X2..X2m.[3..X2m.]3..X2Z.]3+.X2Z.\3..X2Z.[3..X2m.\3.. X2m.Y3..X2..Y2..X2..\3#.X2..]3..X2..X3..X2...2..X2...2..X2..Z3..X2Rich..X2.....PE..L.....\.....!..... .....@.....@.....6..... 7..d.....E.....@..... .....text..... ..`.rdata..8"... ...$.....@..@.data.....P... ...6.....@....r src.....V.....@..@.reloc...E.....F...Z.....@..B..... .....

C:\Users\user\AppData\Local\via-updater\installer.exe	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	72321683
Entropy (8bit):	**7.998222870338434**
Encrypted:	**true**
SSDEEP:	
MD5:	19A1E8AC63BD56062B2E9F0E98AE2B5E
SHA1:	F365277327324417E06EE4A4FDC4FE6E1CEE5614
SHA-256:	4258BA2302FA848BAADE9F9090DE46E367B50A713E21B2707D7721D774A47B53
SHA-512:	4E61B6CAAEB6A9C4CBC58564A596BB3C156FB6A268593A287923005D522F6BE015299F8CDFE5AF689D6730FF7EEDA4F3C880892A96BBEFA67CFFB5D7BE4F544D
Malicious:	false
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...|.oZ.....h...8...@...3.....@..... .....@.....p..... .....text...'f.....h..... ..`.rdata.....l.....@..@.data.....@....ndata.....rsrc.....p.....@..@..... .....

C:\Users\user\AppData\Local\via-updater\installer.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VIA.lnk	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Has Working directory, Icon number=0, Archive, ctime=Fri Feb 12 12:33:42 2021, mtime=Fri Feb 12 12:33:46 2021, atime=Fri Jun 19 02:14:28 2020, length=104941568, window=hide
Category:	dropped
Size (bytes):	4401
Entropy (8bit):	3.705112782532415
Encrypted:	false
SSDEEP:	
MD5:	064F8601C7D505C09FAE64395774AE59
SHA1:	92151A7E33115B72E156AED56E2702947334AD90
SHA-256:	53B35707A81089EF1F041D016B7F620CE0FB9A3FD3D12BC4A8CD9FC805D2D09F
SHA-512:	7B3366CAB087BC916E895832AB7D48F93D076B54F412A976814976756913938626025 10A93ADF296157826BA4EFAA51BC8044703FC169F87F0CCA3E38E97094A
Malicious:	false
Preview:	L.....F.@.. ....g.C...F"n.C.....E...HA.....:..DG..Yr?.D..U..k0.&...&.....-...l.:....x..C.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@. .....Ny.LR.l.....Y.....f.(.A.p.p.D.a.t.a...B.P.1.....LR8l..Local.<.....Ny.LR8l.....Y.....?..L.o.c.a.l.....Z.1.....LR+l..Programs..B.....LR+lLR+l.....g.....P .r.o.g.r.a.m.s.....J.1.....LR5l..via.8.....LR.lLR6l.....h.....B.v.i.a.....V.2..HA..P.. .VIA.exe.@.....LR6lLR8l.....|.....V.I.A...e.x.e.....`.....-....._..... .....XtFu.....C:\Users\user\AppData\Local\Programs\via\VIA.exe..!.Y.e.t. .a.n.o.t.h.e.r. .k.e.y.b.o.a.r.d. .c.o.n.f.i.g.u.r.a.t.o.r.).....\....\....\....\....\.L.o.c.a.l.\.P.r.o.g.r.a.m. s.\.v.i.a.\.V.I.A...e.x.e.).C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.r.o.g.r.a.m.s.\.v.i.a.1.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.r.o.g.r.

C:\Users\user\AppData\Roaming\VIA\.updaterId	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	36
Entropy (8bit):	3.641604167868593
Encrypted:	false
SSDEEP:	
MD5:	B30D903F26C30B223B08AC30E7251420
SHA1:	78F40DE6C4173F53943EDB7793292218B601E1A4
SHA-256:	13B051237A285D9CF091CDCAA18092F7C3ECA615142550F6F2F8C2C17543A969
SHA-512:	6D45D13F023EFFF95138BC7F018ABFC424DA3648F7D1CCF3B39BB931B441F3D20A9EEF62ECE436C34279E68A3B07F7EDDCE4853266EB1DE0CCFED082BF884A AD
Malicious:	false
Preview:	98f005b5-e859-5a9d-90ad-ebea72be1242

C:\Users\user\AppData\Roaming\VIA\64b781ed-dae5-406f-a7cd-fc221f9a4570.tmp	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.619434150836742
Encrypted:	false
SSDEEP:	
MD5:	2800881C775077E1C4B6E06BF4676DE4
SHA1:	2873631068C8B3B9495638C865915BE822442C8B
SHA-256:	226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974
SHA-512:	E342407AB65CC68F1B3FD706CD0A37680A0864FFD30A6539730180EDE2CDCD732CC97AE0B9EF7DB12DA5C0F83E429DF0840DBF7596ACA859A0301665E51737B
Malicious:	false
Preview:	{"net":{"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	ISO-8859 text, with no line terminators, with escape sequences
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CB 0

C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index	
Malicious:	false
Preview:	0\r..m.....

C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index-dir\temp-index	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9972243200613975
Encrypted:	false
SSDEEP:	
MD5:	618C1F2E2859AE0F830E135FABD06799
SHA1:	4F679B053D177505989F8D34F8FA0C2283881AE6
SHA-256:	B172E312A0C70684A98DBE76B12B0B23240FFFA850F50CD297A90E2AC7E7E84B
SHA-512:	463B7BE0CFD23AE6F0EEEDF5C933CC2BA03A812E8801BBBEDD041F044FB4CEB7B17ACAA0DE52CA64ED58F54C07DF8DC6AC1D3550BB087D1BC09D3817653 0DF4
Malicious:	false
Preview:	(...PJ.Zoy retne.....v..../.

C:\Users\user\AppData\Roaming\VIA\GPUCache\data_0	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	FoxPro FPT, blocks size 512, next free block index 3284796609, field type 0
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.01057775872642915
Encrypted:	false
SSDEEP:	
MD5:	CF89D16BB9107C631DAABF0C0EE58EFB
SHA1:	3AE5D3A7CF1F94A56E42F9A58D90A0B9616AE74B
SHA-256:	D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E
SHA-512:	8CB5B059C8105EB91E74A7D5952437AAA1ADA89763C5843E7B0F1B93D9EBE15ED40F287C652229291FAC02D712CF7FF5ECECEF276BA0D7DDC35558A3EC3F7 B0
Malicious:	false
Preview:	.....$..... ....

C:\Users\user\AppData\Roaming\VIA\GPUCache\data_1	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	data
Category:	dropped
Size (bytes):	8488
Entropy (8bit):	0.03491216712472767
Encrypted:	false
SSDEEP:	
MD5:	010587C7093CF69356D298B42109BC7A
SHA1:	F2976E0B433487F6B51D55F7CF62F67B9AC930F7
SHA-256:	A38ABF7CA18924813E8FF2F9003584ABF813F3CF8D24C48B5760CA4F921445FF
SHA-512:	D171754251252C1068DECED2DB41091CCF628BCB92BC6BD981745D77AAEFFDD89D642B2791D1E0C3FC8E9A5EDEBB357B3AC090C999BFD9177A752587052521 F6
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\VIA\GPUCache\data_2	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.011852361981932763
Encrypted:	false

C:\Users\user\AppData\Roaming\VIA\GPUCache\data_2	
SSDEEP:	
MD5:	0962291D6D367570BEE5454721C17E11
SHA1:	59D10A893EF321A706A9255176761366115BEDCB
SHA-256:	EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7
SHA-512:	F555E961B69E09628EAF9C61F465871E6984CD4D31014F954BB747351DAD9CEA6D17C1DB4BCA2C1EB7F187CB5F3C0518748C339C8B43BBD1DBD94AEAA16F58ED
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\VIA\GPUCache\data_3	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.012340643231932763
Encrypted:	false
SSDEEP:	
MD5:	41876349CB12D6DB992F1309F22DF3F0
SHA1:	5CF26B3420FC0302CD0A71E8D029739B8765BE27
SHA-256:	E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C
SHA-512:	E9A4FC1F7CB6AE2901F8E02354A92C4AAA7A53C640DCF692DB42A27A5ACC2A3BFB25A0DE0EB08AB53983132016E7D43132EA4292E439BB636AAFD53FB6EF907E
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\VIA\GPUCache\index	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	FoxPro FPT, blocks size 512, next free block index 3284796353
Category:	dropped
Size (bytes):	368
Entropy (8bit):	0.3511578769559919
Encrypted:	false
SSDEEP:	
MD5:	143BF545C552A0485BF4F783BDEA5743
SHA1:	FC1C02F57154A5D1F85AC792AFCBD22581181636
SHA-256:	0666E68EB536DAE8C7EE5DED4476F3BD90A97A7067B07A2AD22977FAFE90CA3E
SHA-512:	CDA999B74FC0C6BB28D1621E4D633678D5645EF2044BD5A62B35C29F76BF924EA4D3E5903664B049A2395E623E21B97C424769A13C531CE6E4C80A1CE7F830D
Malicious:	false
Preview:	.....p..../..... .....

C:\Users\user\AppData\Roaming\VIA\config.json.1716479925	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	4.696577917905598
Encrypted:	false
SSDEEP:	
MD5:	5D9ABBCA6B0350A8E49DCE2221745DDF
SHA1:	376208C74EC5DDC236D2D4A7DDFFED2C40888C97
SHA-256:	D427B62344C3E1A4DD0BCE5EFBD9D18478635C9C52206F7DE520E37C863DE3CB
SHA-512:	0CCB62D49B570E656D2C62FC3FC3AD7722745C946FFB9108FD01D1B3F82169013F2A0A127F640ECB09971E66EC3758F24E1262CD24AE3EE5DDACBD52C88109
Malicious:	false
Preview:	{.."remoteData": {..."generatedAt": -1,..."definitions": {},..."theme": {...."alpha": {....."c": "#363434",....."t": "#E8C4B8"....},...."mod": {....."c": "#363434",....."t": "#E8C4B8"....},. ..."accent": {....."c": "#E8C4B8",....."t": "#363434"....}...}..},.."settings": {..."allowKeyboardKeyRemapping": false,..."showDesignTab": false,..."disableFastRemap": false,..."disableHardwareAcceleration": false..}.}

C:\Users\user\AppData\Roaming\VIA\logs\main.log	
Process:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	282
Entropy (8bit):	5.007004203518119
Encrypted:	false
SSDEEP:	
MD5:	25DB2451AD6FD5330C954E918203DFEC
SHA1:	FE3B0A9B758506F37DB594514DEA7F7329B5AECC
SHA-256:	6FC205035EAE42F0ADA5203810903B63059B52FCDDE38531EB7C034611EDCE1C
SHA-512:	2D7AAC372FA8334FB72EA2A7C0DDCD1DF2B34A36B68EC40925EFDE91AFB9C8D765927750EA47264B6B88912BA2DBBACCD75A8FB27A43CE67642E30BF77BF8A79
Malicious:	false
Preview:	[2021-02-12 05:34:54.200] [info] Checking for update..[2021-02-12 05:34:54.398] [info] Generated new staging user ID: 98f005b5-e859-5a9d-90ad-ebea72be1242..[2021-02-12 05:36:13.863] [info] Update for version 1.3.1 is not available (latest version: 1.3.1, downgrade is disallowed)...

C:\Users\user\Desktop\VIA.lnk	
Process:	C:\Users\user\Desktop\via-1.3.1-win.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Has Working directory, Icon number=0, Archive, ctime=Fri Feb 12 12:33:42 2021, mtime=Fri Feb 12 12:34:10 2021, atime=Fri Jun 19 02:14:28 2020, length=104941568, window=hide
Category:	modified
Size (bytes):	4385
Entropy (8bit):	3.6951369454780103
Encrypted:	false
SSDEEP:	
MD5:	0BFF41E47F30F35B908E7829A9157CA5
SHA1:	A61148A4E634670C5EF140B36B62B5E6C82F3203
SHA-256:	3027E841D00051CA49F6FA37982C8DE7CB0B0C32C85C7BB631DBFF1F6F2ADA18
SHA-512:	DFC1307B58097941382B191041DD9F346571010514FFAE8BE1A077362CDCCB4E124CB4A9A694A27AC72F3FD93768FD9C1A93BB7BDCC6F1E2F75260A0433BE98
Malicious:	false
Preview:	L.....F.@.. ....g.C.....C.....E...HA.....:..DG..Yr?.D..U..k0.&...&.....-...l..:....x..C.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@. .....Ny.LR.l.....Y.....f.(.A.p.p.D.a.t.a...B.P.1.....LR8l..Local.<.....Ny.LR8l.....Y.....?..L.o.c.a.l.....Z.1.....LR.l..Programs..B.....LR+lLRCl.....g....."...P .r.o.g.r.a.m.s.....J.1.....LRCl..via.8.....LR.lLRCl.....h.....v.i.a.....V.2..HA..P.. .VIA.exe.@.....LR6lLR8l.....|.....V.I.A...e.x.e.....`.....-....._..... ...XtFu.....C:\Users\user\AppData\Local\Programs\via\VIA.exe..!.Y.e.t. .a.n.o.t.h.e.r. .k.e.y.b.o.a.r.d. .c.o.n.f.i.g.u.r.a.t.o.r.%.....\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.r.o.g.r.a.m.s.\.v.i.a.\.V.I.A...e.x.e.).C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.r.o.g.r.a.m.s.\.v.i.a.1.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.P.r.o.g.r.a.m.s.\.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.998222870338434
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:	via-1.3.1-win.exe
File size:	72321683
MD5:	19a1e8ac63bd56062b2e9f0e98ae2b5e
SHA1:	f365277327324417e06ee4a4fdc4fe6e1cee5614
SHA256:	4258ba2302fa848baade9f9090de46e367b50a713e21b207d7721d774a47b53
SHA512:	4e61b6caaeb6a9c4cbc58564a596bb3c156fb6a268593a287923005d522f6be015299f8cdfe5af689d6730ff7eeda4f3c880892a96bbefa67cffb5d7be4f544d
SSDEEP:	1572864:QO9PaiNoZXVp31ent1ZZwMe8L3XRLsgVs6m6aAg5XM5DXkbDI9:Qi+5Vt1Y1ZZwh8NAZ6mrAiXM5DUbq
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...|.oZ.....h...8...@.

File Icon

File Icon

Icon Hash:	21e0c88c52faf804

Static PE Info

General

Entrypoint:	0x40338f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A6FED7C [Tue Jan 30 03:58:52 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 00007F6FA8B076D3h
push ebx
call 00007F6FA8B0A985h
cmp eax, ebx
je 00007F6FA8B076C9h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F6FA8B0A8FFh
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F6FA8B076ACh
push 0000000Ah
call 00007F6FA8B0A958h
push 00000008h

Instruction
call 00007F6FA8B0A951h
push 00000006h
mov dword ptr [0047AEE4h], eax
call 00007F6FA8B0A945h
cmp eax, ebx
je 00007F6FA8B076D1h
push 0000001Eh
call eax
test eax, eax
je 00007F6FA8B076C9h
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	0x8608	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x197000	0x5a5a8	.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	0.66455078125	data	6.4506752227	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x149a	0x1600	False	0.438032670455	data	5.00707518585	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x70ff8	0x600	False	0.518229166667	data	4.03711773145	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x7b000	0x11c000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x197000	0x5a5a8	0x5a600	False	0.0575969268672	data	2.36352325671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1975c8	0x40028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x1d75f0	0x10028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x1e7618	0x4028	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x1eb640	0x2428	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x1eda68	0x1028	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x1eea90	0x928	data	English	United States
RT_ICON	0x1ef3b8	0x428	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x1ef7e0	0x202	data	English	United States
RT_DIALOG	0x1ef9e8	0xf8	data	English	United States
RT_DIALOG	0x1efae0	0xee	data	English	United States
RT_DIALOG	0x1efbd0	0x1fa	data	English	United States
RT_DIALOG	0x1efdd0	0xf0	data	English	United States
RT_DIALOG	0x1efec0	0xe6	data	English	United States
RT_DIALOG	0x1effa8	0x1ee	data	English	United States
RT_DIALOG	0x1f0198	0xe4	data	English	United States
RT_DIALOG	0x1f0280	0xda	data	English	United States
RT_DIALOG	0x1f0360	0x1ee	data	English	United States
RT_DIALOG	0x1f0550	0xe4	data	English	United States
RT_DIALOG	0x1f0638	0xda	data	English	United States
RT_DIALOG	0x1f0718	0x1f2	data	English	United States
RT_DIALOG	0x1f0910	0xe8	data	English	United States
RT_DIALOG	0x1f09f8	0xde	data	English	United States
RT_DIALOG	0x1f0ad8	0x202	data	English	United States
RT_DIALOG	0x1f0ce0	0xf8	data	English	United States
RT_DIALOG	0x1f0dd8	0xee	data	English	United States
RT_GROUP_ICON	0x1f0ec8	0x68	data	English	United States
RT_VERSION	0x1f0f30	0x250	data	English	United States
RT_MANIFEST	0x1f1180	0x423	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

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

Version Infos

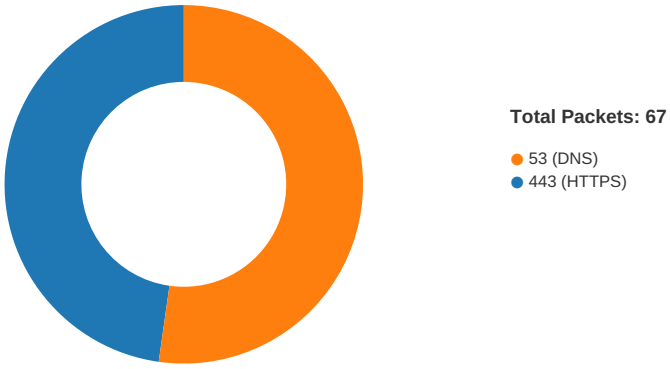
Description	Data
LegalCopyright	Copyright 2020 Olivia
FileVersion	1.3.1
CompanyName	Olivia
ProductName	VIA
ProductVersion	1.3.1
FileDescription	Yet another keyboard configurator
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 05:36:12.394426107 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:12.435436010 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:12.435616970 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:12.437486887 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:12.484029055 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:12.484086990 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:12.484121084 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:12.484164000 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:12.536781073 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.211430073 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.212040901 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.218007088 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.253804922 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.253856897 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.253885984 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.254231930 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.255147934 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.295201063 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.353288889 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421097994 CET	443	49752	140.82.121.4	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 05:36:13.421150923 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421190977 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421219110 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421255112 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421272039 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.421283007 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421323061 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421361923 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421369076 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.421452045 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421484947 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.421535015 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.423825979 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.462460041 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.462522030 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.463802099 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.485187054 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.529162884 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.679414034 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.679466009 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.679513931 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.679552078 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.683034897 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.724080086 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.898838997 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.898890972 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.898922920 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:13.899104118 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.905548096 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:13.948942900 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:14.095691919 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:14.095753908 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:14.095803022 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:14.095829964 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:14.095833063 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:14.095881939 CET	443	49752	140.82.121.4	192.168.2.3
Feb 12, 2021 05:36:14.096167088 CET	49752	443	192.168.2.3	140.82.121.4
Feb 12, 2021 05:36:14.163393974 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.206959009 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.207083941 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.207901955 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.251291037 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.252448082 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.252494097 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.252532959 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.252563000 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.252634048 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.252671957 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.276770115 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.277121067 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.277405024 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.322140932 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.322190046 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.323008060 CET	49753	443	192.168.2.3	185.199.111.154
Feb 12, 2021 05:36:14.413923025 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.426830053 CET	443	49753	185.199.111.154	192.168.2.3
Feb 12, 2021 05:36:14.479727983 CET	49753	443	192.168.2.3	185.199.111.154

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 05:33:01.721486092 CET	58361	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:01.772696972 CET	53	58361	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:03.781474113 CET	63492	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 05:33:03.830204964 CET	53	63492	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:05.153208017 CET	60831	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:05.202788115 CET	53	60831	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:05.983519077 CET	60100	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:06.034789085 CET	53	60100	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:11.990360022 CET	53195	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:12.039210081 CET	53	53195	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:21.940181971 CET	50141	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:21.997534037 CET	53	50141	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:23.631787062 CET	53023	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:23.680524111 CET	53	53023	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:24.464355946 CET	49563	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:24.524189949 CET	53	49563	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:25.745594025 CET	51352	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:25.797029018 CET	53	51352	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:27.008279085 CET	59349	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:27.057795048 CET	53	59349	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:28.003413916 CET	57084	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:28.062118053 CET	53	57084	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:29.243135929 CET	58823	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:29.291896105 CET	53	58823	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:35.211301088 CET	57568	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:35.225122929 CET	50540	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:35.273875952 CET	53	50540	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:35.294302940 CET	53	57568	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:50.730648041 CET	54366	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:50.781121969 CET	53	54366	8.8.8.8	192.168.2.3
Feb 12, 2021 05:33:59.029803038 CET	53034	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:33:59.090914011 CET	53	53034	8.8.8.8	192.168.2.3
Feb 12, 2021 05:34:08.205447912 CET	57762	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:34:08.273072958 CET	53	57762	8.8.8.8	192.168.2.3
Feb 12, 2021 05:34:39.279285908 CET	55435	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:34:39.328164101 CET	53	55435	8.8.8.8	192.168.2.3
Feb 12, 2021 05:34:43.123123884 CET	50713	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:34:43.184216022 CET	53	50713	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:14.976568937 CET	56132	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:15.029881954 CET	53	56132	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:16.705853939 CET	58987	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:16.775979042 CET	53	58987	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:53.999831915 CET	56579	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:54.059849977 CET	53	56579	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:54.746124983 CET	60633	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:54.806022882 CET	53	60633	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:55.627259016 CET	61292	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:55.677222967 CET	53	61292	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:56.392687082 CET	63619	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:56.441499949 CET	53	63619	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:57.151278973 CET	64938	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:57.211365938 CET	53	64938	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:57.907037973 CET	61946	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:57.955928087 CET	53	61946	8.8.8.8	192.168.2.3
Feb 12, 2021 05:35:58.804889917 CET	64910	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:35:58.853718996 CET	53	64910	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:00.042251110 CET	52123	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:36:00.099704027 CET	53	52123	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:01.362181902 CET	56130	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:36:01.422182083 CET	53	56130	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:02.062622070 CET	56338	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:36:02.122375011 CET	53	56338	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:12.315362930 CET	62938	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:36:12.387630939 CET	53	62938	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:14.111283064 CET	55708	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:36:14.161325932 CET	53	55708	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:41.548944950 CET	58306	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 05:36:41.621475935 CET	53	58306	8.8.8.8	192.168.2.3
Feb 12, 2021 05:36:41.848463058 CET	64124	53	192.168.2.3	8.8.8.8
Feb 12, 2021 05:36:41.913203955 CET	53	64124	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 12, 2021 05:36:12.315362930 CET	192.168.2.3	8.8.8.8	0xc8a8	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:14.111283064 CET	192.168.2.3	8.8.8.8	0x906f	Standard query (0)	github-releases.githubusercontent.com	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:41.548944950 CET	192.168.2.3	8.8.8.8	0x8afc	Standard query (0)	www.caniusevia.com	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:41.848463058 CET	192.168.2.3	8.8.8.8	0xc9bf	Standard query (0)	caniusevia.com	A (IP address)	IN (0x0001)

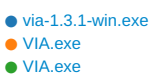
DNS Answers

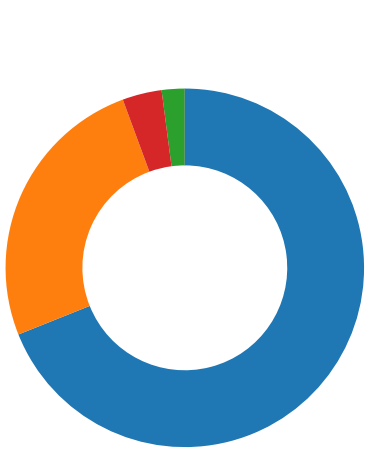
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 12, 2021 05:36:12.387630939 CET	8.8.8.8	192.168.2.3	0xc8a8	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:14.161325932 CET	8.8.8.8	192.168.2.3	0x906f	No error (0)	github-releases.githubusercontent.com		185.199.111.154	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:14.161325932 CET	8.8.8.8	192.168.2.3	0x906f	No error (0)	github-releases.githubusercontent.com		185.199.108.154	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:14.161325932 CET	8.8.8.8	192.168.2.3	0x906f	No error (0)	github-releases.githubusercontent.com		185.199.110.154	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:14.161325932 CET	8.8.8.8	192.168.2.3	0x906f	No error (0)	github-releases.githubusercontent.com		185.199.109.154	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:41.621475935 CET	8.8.8.8	192.168.2.3	0x8afc	No error (0)	www.caniusevia.com		18.198.68.141	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:41.621475935 CET	8.8.8.8	192.168.2.3	0x8afc	No error (0)	www.caniusevia.com		134.209.226.211	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:41.913203955 CET	8.8.8.8	192.168.2.3	0xc9bf	No error (0)	caniusevia.com		167.99.137.12	A (IP address)	IN (0x0001)
Feb 12, 2021 05:36:41.913203955 CET	8.8.8.8	192.168.2.3	0xc9bf	No error (0)	caniusevia.com		142.93.108.123	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





System Behavior

Analysis Process: via-1.3.1-win.exe PID: 4084 Parent PID: 5568

General

Start time:	05:33:19
Start date:	12/02/2021
Path:	C:\Users\user\Desktop\via-1.3.1-win.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\via-1.3.1-win.exe'
Imagebase:	0x400000
File size:	72321683 bytes
MD5 hash:	19A1E8AC63BD56062B2E9F0E98AE2B5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsmBD1E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E1E	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E1E	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40583A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	8	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\StdUtils.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\SpiderBanner.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	244	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\StdUtils.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	5	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40587A	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40587A	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40587A	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40587A	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsis7z.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\resources	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\swiftshader	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\chrome_100_percent.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\chrome_200_percent.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\icudtl.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\LICENSE.electron.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\LICENSES.chromium.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	53	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\locales\am.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ar.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\bg.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\bn.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ca.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\cs.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\da.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\de.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\el.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\en-GB.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\en-US.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\es-419.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\es.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\et.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\fa.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\fi.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\fil.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\fr.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\gu.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\he.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\hi.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\hr.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\hu.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\id.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\it.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ja.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\kn.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ko.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\lt.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\lv.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ml.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\mr.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ms.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\nb.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\nl.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\pl.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\pt-BR.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\pt-PT.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ro.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ru.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\sk.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\sl.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\sr.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\sv.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\sw.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\ta.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\te.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\th.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\tr.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\uk.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\vi.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\zh-CN.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\locales\zh-TW.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\natives_blob.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\resources.pak	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\resources	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\resources\app-update.yml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\snapshot_blob.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\v8_context_snapshot.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\ffmpeg.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\libEGL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\libGLESv2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\resources	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\swiftshader	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7028051A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\swiftshader\libEGL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\swiftshader\libGLESv2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\Programs\via\VIA.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	70280FD9	CreateFileW
C:\Users\user\AppData\Local\via-updater	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40587A	CreateDirectoryW
C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\WinShell.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\WinShell.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	405DDC	CreateFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	405DDC	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmBD1E.tmp	success or wait	1	40363E	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp	success or wait	1	4059FB	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	success or wait	1	4059AD	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsis7z.dll	success or wait	1	4059AD	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	cannot delete	1	4059AD	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\SpiderBanner.dll	success or wait	1	4059AD	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\StdUtils.dll	success or wait	1	4059AD	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	success or wait	1	4059AD	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\WinShell.dll	success or wait	1	4059AD	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 71 72 2a 92 35 13 44 c1 35 13 44 c1 35 13 44 c1 b6 0f 4a c1 32 13 44 c1 35 13 45 c1 21 13 44 c1 f6 1c 19 c1 32 13 44 c1 61 30 74 c1 31 13 44 c1 56 31 6e c1 34 13 44 c1 ca 33 40 c1 34 13 44 c1 52 69 63 68 35 13 44 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 15 ed 6f 5a 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 97 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......qr*.5.D.5.D.5.D...J.2. D.5.E.!.D.....2.D.a0t.1.D.V1 n. 4.D..3@.4.D.Rich5.D......... PE..L.....oZ...........!..... .. ..).....	success or wait	1	405E7C	WriteFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\StdUtils.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 c4 a7 71 10 80 c6 1f 43 80 c6 1f 43 80 c6 1f 43 89 be 8c 43 90 c6 1f 43 80 c6 1e 43 ea c6 1f 43 ef d9 1b 43 83 c6 1f 43 03 da 11 43 84 c6 1f 43 89 be 9c 43 83 c6 1f 43 9b 5b b0 43 99 c6 1f 43 9b 5b 84 43 81 c6 1f 43 9b 5b 85 43 81 c6 1f 43 9b 5b 82 43 81 c6 1f 43 52 69 63 68 80 c6 1f 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	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.[.C...CRich...C................ ........PE..L..	success or wait	5	405E7C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\SpiderBanner.dll	unknown	9216	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 e1 4e 84 84 a5 2f ea d7 a5 2f ea d7 a5 2f ea d7 ac 57 79 d7 a2 2f ea d7 a5 2f eb d7 94 2f ea d7 f1 0c da d7 a4 2f ea d7 ac 57 69 d7 a7 2f ea d7 ac 57 78 d7 a4 2f ea d7 ac 57 7e d7 a4 2f ea d7 ac 57 7b d7 a4 2f ea d7 52 69 63 68 a5 2f ea d7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 54 7b 6d 57 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 14 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........N.../.../.../...Wy../ .../.../......./...Wi../...Wx. ./...W~../...W{../..Rich./.... ..............PE..L...T{mW.... ....!.......	success or wait	1	405E7C	WriteFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	unknown	4608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 0d da 73 cf 49 bb 1d 9c 49 bb 1d 9c 49 bb 1d 9c 6e 7d 66 9c 4c bb 1d 9c 49 bb 1c 9c 50 bb 1d 9c 40 c3 9e 9c 4b bb 1d 9c 40 c3 8f 9c 48 bb 1d 9c 40 c3 8c 9c 48 bb 1d 9c 52 69 63 68 49 bb 1d 9c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5c 87 09 4e 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 06 00 00 00 08 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.........s.I...I...I...n}f.L. ..I...P...@...K...@...H...@... H...RichI..................... ......PE..L...\..N...........!	success or wait	1	405E7C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	32768	37 7a bc af 27 1c 00 04 aa 42 9b 2c 47 78 42 04 00 00 00 00 25 00 00 00 00 00 00 00 b2 06 83 93 e0 c7 39 c0 04 5d 00 02 80 36 bf 96 d2 ac b4 7a 61 8e ac f7 e3 c5 e3 40 00 38 19 cc 71 68 e8 c8 b5 9a 6a d9 d6 85 5c 45 64 94 20 62 9f 45 1e b1 f0 81 9b 9c 6a df d8 d5 22 89 34 5c a3 c0 db e7 5c 13 e2 3a 48 30 ae d1 ba cd 32 38 6d 15 f5 a7 fb 9f 44 92 4b 94 86 6e b2 d3 7d dd 40 1b 3b a1 b3 a6 d1 22 1c 16 6b 43 70 8a db d8 e2 be a7 94 d5 52 78 e4 c0 6b 8d 14 e1 e6 bd 8d 1f 76 a9 45 7e e4 57 49 3d 83 b6 85 6e ab c8 1a 5c 2a 08 f3 35 87 0b bb f4 bd 2d 43 db c9 34 0d fd b5 6d a9 7b 29 94 bd 2e c3 fe dd c2 11 04 c5 43 aa c8 c6 dc 53 f7 5f 13 bd de 65 0a 33 b4 5c 65 33 5e 79 3d 91 09 02 c3 30 e4 db 9e 25 8d c4 0e 4d 41 8f f1 a3 0a 3e 9c 64 e6 84 77 a4 da e6 ae 8f 46	7z..'....B.,GxB.....%......... ....9..]...6.....za......@.8.. qh....j...\Ed. b.E......j...". 4\....\..:H0....28m.....D.K..n ..}.@.;...."..kCp........Rx..k ....v.E~.WI=...n...*..5.....- C..4...m.{}..........C....S ._...e.3.\e3^y=....0...%...MA ....>.d..w.....F	success or wait	2181	405E7C	WriteFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsis7z.dll	unknown	23640	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 4c 9d 36 61 08 fc 58 32 08 fc 58 32 08 fc 58 32 6d 9a 5b 33 04 fc 58 32 6d 9a 5d 33 90 fc 58 32 5a 94 5d 33 2b fc 58 32 5a 94 5c 33 18 fc 58 32 5a 94 5b 33 1c fc 58 32 6d 9a 5c 33 1b fc 58 32 6d 9a 59 33 07 fc 58 32 08 fc 59 32 b6 fc 58 32 9a 95 5c 33 23 fc 58 32 9a 95 5d 33 8b fc 58 32 9a 95 58 33 09 fc 58 32 9a 95 a7 32 09 fc 58 32 08 fc cf 32 09 fc 58 32 9a 95 5a 33 09 fc 58	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......L.6a..X2..X2..X2m. [3.. X2m.]3..X2Z.]3+.X2Z.\3..X 2Z.[3 ..X2m.\3..X2m.Y3..X2..Y2.. X2.. \3#.X2..]3..X2..X3..X2...2.. X2...2..X2..Z3..X	success or wait	17	405E7C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\chrome_100_percent.pak	unknown	177830	05 00 00 00 01 00 00 00 af 00 1a 00 18 01 94 04 00 00 f8 43 f2 05 00 00 f9 43 b8 07 00 00 fa 43 1a 0b 00 00 fb 43 a5 0d 00 00 fc 43 37 0f 00 00 fd 43 e2 0f 00 00 fe 43 ef 12 00 00 ff 43 96 15 00 00 00 44 90 17 00 00 01 44 cb 1a 00 00 07 44 35 1d 00 00 08 44 df 1e 00 00 0a 44 1a 20 00 00 0c 44 41 21 00 00 0d 44 f3 22 00 00 14 44 8e 23 00 00 15 44 ec 2c 00 00 38 63 1b 2f 00 00 39 63 3c 30 00 00 3a 63 fc 31 00 00 3b 63 e4 34 00 00 3c 63 dd 37 00 00 00 64 a7 3b 00 00 01 64 b9 3c 00 00 02 64 4a 3e 00 00 03 64 9f 3f 00 00 04 64 92 40 00 00 05 64 34 41 00 00 64 64 d6 41 00 00 65 64 4a 83 00 00 66 64 a7 8d 00 00 78 69 7c 90 00 00 79 69 81 92 00 00 7a 69 b7 9b 00 00 7b 69 b4 9d 00 00 7c 69 ef a0 00 00 7d 69 1c a6 00 00 7e 69 89 af 00 00 81 69 35 b1 00 00 82 69 1a	.....C.....C.....C.....C.....C.....C7....C.....C.....C.....D.....D.....D5....D.... .D. ...DA!...D."...D.#...D.,..8c./..9c<0..:c.1..;c.4..<c.7..d.;...d.<...dJ>...d.?...d.@..d4A..dd.A..edJ...fd....xi|...yi....zi....{i....|i....}i....~i.....i5....i.	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\chrome_200_percent.pak	unknown	315644	05 00 00 00 01 00 00 00 b2 00 17 00 18 01 9a 04 00 00 f8 43 f3 06 00 00 f9 43 02 0b 00 00 fa 43 e6 12 00 00 fb 43 ab 18 00 00 fc 43 e9 1b 00 00 fd 43 e4 1c 00 00 fe 43 a2 23 00 00 ff 43 de 28 00 00 00 44 ee 2b 00 00 01 44 5e 33 00 00 07 44 9b 37 00 00 08 44 f3 39 00 00 0a 44 81 3b 00 00 0c 44 05 3d 00 00 0d 44 55 40 00 00 14 44 ff 40 00 00 15 44 78 55 00 00 38 63 ad 5a 00 00 39 63 98 5e 00 00 3a 63 c2 61 00 00 3b 63 b6 64 00 00 3c 63 bb 67 00 00 00 64 91 6b 00 00 01 64 a3 6c 00 00 02 64 34 6e 00 00 03 64 89 6f 00 00 04 64 7c 70 00 00 05 64 1e 71 00 00 64 64 c0 71 00 00 65 64 34 b3 00 00 66 64 91 bd 00 00 78 69 66 c0 00 00 79 69 09 c5 00 00 7a 69 4b ce 00 00 7b 69 54 d0 00 00 7c 69 9b d3 00 00 7d 69 d4 d8 00 00 7e 69 4d e2 00 00 81 69 05 e4 00 00 82 69 f6	.....C.....C.....C.....C.....C.....C.#..C.(...D.+...D^3...D.7...D.9..D.;...D.=...DU@...D.@...DxU..8c.Z..9c.^..:c.a..;c.d..<c.g..d.k...d.l...d4n...d.o...d|p..d.q..dd.q..ed4...fd....xif...yi....ziK...{iT...|i....}i....~iM....i.....i.	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\icudtl.dat	unknown	1048576	90 00 da 27 14 00 00 00 00 00 02 00 43 6d 6e 44 01 00 00 00 03 00 00 00 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 32 30 31 36 20 61 6e 64 20 6c 61 74 65 72 3a 20 55 6e 69 63 6f 64 65 2c 20 49 6e 63 2e 20 61 6e 64 20 6f 74 68 65 72 73 2e 20 4c 69 63 65 6e 73 65 20 26 20 74 65 72 6d 73 20 6f 66 20 75 73 65 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 75 6e 69 63 6f 64 65 2e 6f 72 67 2f 63 6f 70 79 72 69 67 68 74 2e 68 74 6d 6c 20 00 2e 05 00 00 74 29 00 00 c0 9b 00 00 84 29 00 00 10 9c 00 00 94 29 00 00 60 9c 00 00 a4 29 00 00 60 c4 00 00 b4 29 00 00 c0 c4 00 00 c4 29 00 00 60 0b 01 00 d8 29 00 00 b0 0b 01 00 eb 29 00 00 e0 0c 01 00 fe 29 00 00 70 0d 01 00 11 2a 00 00 d0 0d 01 00 24 2a 00 00 a0 0f 01 00 37 2a 00 00 30 10 01 00 4a 2a 00 00 90 10 01 00 5d 2a 00	...'.....CmnD..... Copyright (C) 2016 and later: Unicode, Inc. and others. License & terms of use: http://www.unicode.org/copyright.html .....t).....).....)..`....)..`....)..`....)..`....)....)..p....*.....$*.....7*..0...J*.....]*.	success or wait	10	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\LICENSE.electron.txt	unknown	1060	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30 31 33 2d 32 30 31 39 20 47 69 74 48 75 62 20 49 6e 63 2e 0a 0a 50 65 72 6d 69 73 73 69 6f 6e 20 69 73 20 68 65 72 65 62 79 20 67 72 61 6e 74 65 64 2c 20 66 72 65 65 20 6f 66 20 63 68 61 72 67 65 2c 20 74 6f 20 61 6e 79 20 70 65 72 73 6f 6e 20 6f 62 74 61 69 6e 69 6e 67 0a 61 20 63 6f 70 79 20 6f 66 20 74 68 69 73 20 73 6f 66 74 77 61 72 65 20 61 6e 64 20 61 73 73 6f 63 69 61 74 65 64 20 64 6f 63 75 6d 65 6e 74 61 74 69 6f 6e 20 66 69 6c 65 73 20 28 74 68 65 0a 22 53 6f 66 74 77 61 72 65 22 29 2c 20 74 6f 20 64 65 61 6c 20 69 6e 20 74 68 65 20 53 6f 66 74 77 61 72 65 20 77 69 74 68 6f 75 74 20 72 65 73 74 72 69 63 74 69 6f 6e 2c 20 69 6e 63 6c 75 64 69 6e 67 0a 77 69 74 68 6f 75 74 20 6c 69 6d 69 74 61 74 69	Copyright (c) 2013-2019 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 limitati	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\LICENSES.chromium.html	unknown	1048576	3c 21 2d 2d 20 47 65 6e 65 72 61 74 65 64 20 62 79 20 6c 69 63 65 6e 73 65 73 2e 70 79 3b 20 64 6f 20 6e 6f 74 20 65 64 69 74 2e 20 2d 2d 3e 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0d 0a 3c 74 69 74 6c 65 3e 43 72 65 64 69 74 73 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 68 72 6f 6d 65 3a 2f 2f 72 65 73 6f 75 72 63 65 73 2f 63 73 73 2f 74 65 78 74 5f 64 65 66 61 75 6c 74 73 2e 63 73 73 22 3e 0d 0a 3c	Generated by licenses.py; do not edit. --><!doctype html>..<html>..<head>..<meta charset="utf-8">..<meta name="viewport" content="width=device-width">..<title>Credits</title>..<link rel="stylesheet" href="chrome://resources/css/text_defaults.css">..<	success or wait	5	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\am.pak	unknown	122392	05 00 00 00 01 00 00 00 a2 06 c5 00 7c 00 f2 2a 00 00 7d 00 01 2b 00 00 7e 00 0c 2b 00 00 80 00 14 2b 00 00 81 00 19 2b 00 00 82 00 26 2b 00 00 83 00 2c 2b 00 00 84 00 3b 2b 00 00 85 00 4c 2b 00 00 86 00 55 2b 00 00 88 00 6a 2b 00 00 89 00 77 2b 00 00 8b 00 7d 2b 00 00 8c 00 8c 2b 00 00 8e 00 92 2b 00 00 8f 00 a4 2b 00 00 91 00 ac 2b 00 00 92 00 b1 2b 00 00 94 00 b9 2b 00 00 9d 00 c1 2b 00 00 9e 00 c9 2b 00 00 9f 00 d0 2b 00 00 a0 00 d7 2b 00 00 a3 00 de 2b 00 00 a4 00 df 2b 00 00 a6 00 e0 2b 00 00 a7 00 fc 2b 00 00 a8 00 12 2c 00 00 b1 00 41 2c 00 00 b4 00 60 2c 00 00 b5 00 7f 2c 00 00 b6 00 8b 2c 00 00 b7 00 94 2c 00 00 b8 00 b0 2c 00 00 bc 00 b6 2c 00 00 bd 00 bd 2c 00 00 be 00 c0 2c 00 00 bf 00 c1 2c 00 00 c0 00 c8 2c 00 00 c2 00 df 2c 00 00 c5 00 eb	.....|..*..}..+..~..+.. ...+.....+....&+....,+....;+.. ..L+....U+....j+....w+....}+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ..A,....`,.....,.....,.....,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\ar.pak	unknown	123569	05 00 00 00 01 00 00 00 a1 06 c6 00 7c 00 f0 2a 00 00 7d 00 ff 2a 00 00 7e 00 0a 2b 00 00 80 00 12 2b 00 00 81 00 17 2b 00 00 82 00 24 2b 00 00 83 00 2a 2b 00 00 84 00 39 2b 00 00 85 00 4a 2b 00 00 86 00 53 2b 00 00 88 00 68 2b 00 00 89 00 75 2b 00 00 8b 00 7b 2b 00 00 8c 00 8a 2b 00 00 8e 00 90 2b 00 00 8f 00 a2 2b 00 00 91 00 aa 2b 00 00 92 00 af 2b 00 00 94 00 b7 2b 00 00 9d 00 bf 2b 00 00 9e 00 c7 2b 00 00 9f 00 ce 2b 00 00 a0 00 d5 2b 00 00 a3 00 dc 2b 00 00 a6 00 de 2b 00 00 a7 00 f7 2b 00 00 a8 00 14 2c 00 00 b1 00 4b 2c 00 00 b4 00 64 2c 00 00 b5 00 96 2c 00 00 b6 00 a0 2c 00 00 b7 00 aa 2c 00 00 b8 00 b8 2c 00 00 bc 00 c2 2c 00 00 bd 00 c9 2c 00 00 bf 00 cc 2c 00 00 c0 00 d3 2c 00 00 c2 00 e9 2c 00 00 c5 00 09 2d 00 00 ce 00 1c 2d 00 00 dc 00 3c	.....|..*..}..*..~..+.. ...+.....+....$+....*+....9+.. ..J+....S+....h+....u+....{+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,....K,.. ..d,.....,.....,.....,..... ...,.....,.....,.....,.....,.....-.....-....<	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\bg.pak	unknown	133078	05 00 00 00 01 00 00 00 b1 06 b6 00 7c 00 10 2b 00 00 7d 00 1f 2b 00 00 7e 00 2a 2b 00 00 80 00 32 2b 00 00 81 00 37 2b 00 00 82 00 44 2b 00 00 83 00 4a 2b 00 00 84 00 59 2b 00 00 85 00 6a 2b 00 00 86 00 73 2b 00 00 88 00 88 2b 00 00 89 00 95 2b 00 00 8b 00 9b 2b 00 00 8c 00 aa 2b 00 00 8e 00 b0 2b 00 00 8f 00 c2 2b 00 00 91 00 ca 2b 00 00 92 00 cf 2b 00 00 94 00 d7 2b 00 00 9d 00 df 2b 00 00 9e 00 e7 2b 00 00 9f 00 ee 2b 00 00 a0 00 f5 2b 00 00 a3 00 fc 2b 00 00 a4 00 fd 2b 00 00 a6 00 fe 2b 00 00 a7 00 20 2c 00 00 a8 00 39 2c 00 00 b1 00 56 2c 00 00 b4 00 99 2c 00 00 b5 00 be 2c 00 00 b6 00 d2 2c 00 00 b7 00 e8 2c 00 00 b8 00 04 2d 00 00 bc 00 16 2d 00 00 bd 00 1d 2d 00 00 be 00 20 2d 00 00 bf 00 21 2d 00 00 c0 00 32 2d 00 00 c2 00 55 2d 00 00 c5 00 5f	.....|..+..}..+..~.*+.. ..2+....7+....D+....J+....Y+.. ..j+....s+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.... ,....9,.. ..V,.....,.....,.....,.....-.....-.....-.... -....!-....2-....U-...._	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\bn.pak	unknown	173570	05 00 00 00 01 00 00 00 a2 06 c5 00 7c 00 f2 2a 00 00 7d 00 01 2b 00 00 7e 00 0c 2b 00 00 80 00 14 2b 00 00 81 00 1a 2b 00 00 82 00 27 2b 00 00 83 00 2d 2b 00 00 84 00 3c 2b 00 00 85 00 4d 2b 00 00 86 00 56 2b 00 00 88 00 6b 2b 00 00 89 00 78 2b 00 00 8b 00 7e 2b 00 00 8c 00 8d 2b 00 00 8e 00 93 2b 00 00 8f 00 a5 2b 00 00 91 00 ad 2b 00 00 92 00 b2 2b 00 00 94 00 ba 2b 00 00 98 00 c2 2b 00 00 9d 00 c7 2b 00 00 9e 00 cf 2b 00 00 9f 00 d6 2b 00 00 a0 00 dd 2b 00 00 a3 00 e4 2b 00 00 a4 00 e5 2b 00 00 a6 00 e6 2b 00 00 a7 00 0b 2c 00 00 a8 00 30 2c 00 00 b1 00 5b 2c 00 00 b4 00 83 2c 00 00 b5 00 c0 2c 00 00 b6 00 d6 2c 00 00 b7 00 e9 2c 00 00 b8 00 14 2d 00 00 bd 00 20 2d 00 00 be 00 23 2d 00 00 bf 00 24 2d 00 00 c0 00 3b 2d 00 00 c2 00 5c 2d 00 00 c5 00 6b	.....|..*..}..+..~..+.. ...+.....+....'+....-+....<+.. ..M+....V+....k+....x+....~+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,....0,.... [,.....,.....,.....,.....,.....-.... - ....#-....$-....;-....\-....k	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\ca.pak	unknown	87098	05 00 00 00 01 00 00 00 ae 06 b9 00 7c 00 0a 2b 00 00 7d 00 19 2b 00 00 7e 00 24 2b 00 00 80 00 2c 2b 00 00 81 00 31 2b 00 00 82 00 3e 2b 00 00 83 00 44 2b 00 00 84 00 53 2b 00 00 85 00 64 2b 00 00 86 00 6d 2b 00 00 88 00 82 2b 00 00 89 00 8f 2b 00 00 8b 00 95 2b 00 00 8c 00 a4 2b 00 00 8e 00 aa 2b 00 00 8f 00 bc 2b 00 00 91 00 c4 2b 00 00 92 00 c9 2b 00 00 94 00 d1 2b 00 00 9d 00 d9 2b 00 00 9e 00 e1 2b 00 00 9f 00 e8 2b 00 00 a0 00 ef 2b 00 00 a3 00 f6 2b 00 00 a4 00 f7 2b 00 00 a6 00 f8 2b 00 00 a7 00 12 2c 00 00 a8 00 2b 2c 00 00 b1 00 4b 2c 00 00 b4 00 66 2c 00 00 b5 00 84 2c 00 00 b6 00 8d 2c 00 00 b7 00 96 2c 00 00 b8 00 9e 2c 00 00 bc 00 a3 2c 00 00 bd 00 aa 2c 00 00 be 00 ad 2c 00 00 bf 00 ae 2c 00 00 c0 00 b4 2c 00 00 c2 00 c6 2c 00 00 c5 00 cc	.....|..+..}..+..~.$+.. ..,+....1+....>+....D+....S+.. ..d+....m+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,....+,.. ..K,....f,.....,.....,.....,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\cs.pak	unknown	88849	05 00 00 00 01 00 00 00 ab 06 bc 00 7c 00 04 2b 00 00 7d 00 13 2b 00 00 7e 00 1e 2b 00 00 80 00 26 2b 00 00 81 00 2b 2b 00 00 82 00 38 2b 00 00 83 00 3e 2b 00 00 84 00 4d 2b 00 00 85 00 5e 2b 00 00 86 00 67 2b 00 00 88 00 7c 2b 00 00 89 00 89 2b 00 00 8b 00 8f 2b 00 00 8c 00 9e 2b 00 00 8e 00 a4 2b 00 00 8f 00 b6 2b 00 00 91 00 be 2b 00 00 92 00 c3 2b 00 00 94 00 cb 2b 00 00 9d 00 d3 2b 00 00 9e 00 db 2b 00 00 9f 00 e2 2b 00 00 a0 00 e9 2b 00 00 a3 00 f0 2b 00 00 a4 00 f1 2b 00 00 a6 00 f2 2b 00 00 a7 00 02 2c 00 00 a8 00 14 2c 00 00 b1 00 26 2c 00 00 b4 00 3f 2c 00 00 b5 00 54 2c 00 00 b6 00 61 2c 00 00 b7 00 6e 2c 00 00 b8 00 75 2c 00 00 bc 00 7d 2c 00 00 bd 00 84 2c 00 00 be 00 87 2c 00 00 bf 00 88 2c 00 00 c0 00 93 2c 00 00 c2 00 9f 2c 00 00 c5 00 a4	.....|..+..}..+..~..+.. ..&+....++....8+....>+....M+.. ..^+....g+....|+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..&,....?,....T,....a,....n,.. ..u,....},.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\da.pak	unknown	80484	05 00 00 00 01 00 00 00 b1 06 b6 00 7c 00 10 2b 00 00 7d 00 1f 2b 00 00 7e 00 2a 2b 00 00 80 00 32 2b 00 00 81 00 37 2b 00 00 82 00 44 2b 00 00 83 00 4a 2b 00 00 84 00 59 2b 00 00 85 00 6a 2b 00 00 86 00 73 2b 00 00 88 00 88 2b 00 00 89 00 95 2b 00 00 8b 00 9b 2b 00 00 8c 00 aa 2b 00 00 8e 00 b0 2b 00 00 8f 00 c2 2b 00 00 91 00 ca 2b 00 00 92 00 cf 2b 00 00 94 00 d7 2b 00 00 9d 00 df 2b 00 00 9e 00 e7 2b 00 00 9f 00 ee 2b 00 00 a0 00 f5 2b 00 00 a3 00 fc 2b 00 00 a4 00 fd 2b 00 00 a6 00 fe 2b 00 00 a7 00 0c 2c 00 00 a8 00 1c 2c 00 00 b1 00 30 2c 00 00 b4 00 3f 2c 00 00 b5 00 58 2c 00 00 b6 00 5f 2c 00 00 b7 00 68 2c 00 00 b8 00 6e 2c 00 00 bc 00 71 2c 00 00 bd 00 78 2c 00 00 be 00 7b 2c 00 00 bf 00 7c 2c 00 00 c0 00 83 2c 00 00 c2 00 8e 2c 00 00 c5 00 95	.....|..+..}..+..~.*+.. ..2+....7+....D+....J+....Y+.. ..j+....s+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..0,....?,....X,....._,....h,.. ..n,....q,....x,....{,.....|,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\de.pak	unknown	86153	05 00 00 00 01 00 00 00 9e 06 c9 00 7c 00 ea 2a 00 00 7d 00 f9 2a 00 00 7e 00 04 2b 00 00 80 00 0c 2b 00 00 81 00 11 2b 00 00 82 00 1e 2b 00 00 83 00 24 2b 00 00 84 00 33 2b 00 00 85 00 44 2b 00 00 86 00 4d 2b 00 00 88 00 62 2b 00 00 89 00 6f 2b 00 00 8b 00 75 2b 00 00 8c 00 84 2b 00 00 8e 00 8a 2b 00 00 8f 00 9c 2b 00 00 91 00 a4 2b 00 00 92 00 a9 2b 00 00 94 00 b1 2b 00 00 9d 00 b9 2b 00 00 9e 00 c1 2b 00 00 9f 00 c8 2b 00 00 a0 00 cf 2b 00 00 a3 00 d6 2b 00 00 a4 00 d7 2b 00 00 a6 00 d8 2b 00 00 a7 00 e9 2b 00 00 a8 00 fc 2b 00 00 b1 00 0e 2c 00 00 b4 00 1e 2c 00 00 b5 00 34 2c 00 00 b6 00 3f 2c 00 00 b7 00 4b 2c 00 00 b8 00 5b 2c 00 00 bc 00 65 2c 00 00 bd 00 6c 2c 00 00 be 00 6f 2c 00 00 bf 00 70 2c 00 00 c0 00 79 2c 00 00 c2 00 8a 2c 00 00 c5 00 91	.....|..*..}..*..~..+.. ...+.....+.....+....$+....3+.. ..D+....M+....b+....o+....u+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,....4,....?,....K,.... [,....e,....l,....o,....p,.. ..y,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\el.pak	unknown	148899	05 00 00 00 01 00 00 00 a3 06 c4 00 7c 00 f4 2a 00 00 7d 00 03 2b 00 00 7e 00 0e 2b 00 00 80 00 16 2b 00 00 81 00 1b 2b 00 00 82 00 28 2b 00 00 83 00 2e 2b 00 00 84 00 3d 2b 00 00 85 00 4e 2b 00 00 86 00 57 2b 00 00 88 00 6c 2b 00 00 89 00 79 2b 00 00 8b 00 7f 2b 00 00 8c 00 8e 2b 00 00 8e 00 94 2b 00 00 8f 00 a6 2b 00 00 91 00 ae 2b 00 00 92 00 b3 2b 00 00 94 00 bb 2b 00 00 9d 00 c3 2b 00 00 9e 00 cb 2b 00 00 9f 00 d2 2b 00 00 a0 00 d9 2b 00 00 a3 00 e0 2b 00 00 a4 00 e1 2b 00 00 a6 00 e2 2b 00 00 a7 00 09 2c 00 00 a8 00 2e 2c 00 00 b1 00 68 2c 00 00 b4 00 91 2c 00 00 b5 00 ca 2c 00 00 b6 00 e6 2c 00 00 b7 00 00 2d 00 00 b8 00 12 2d 00 00 bc 00 22 2d 00 00 bd 00 29 2d 00 00 be 00 2c 2d 00 00 bf 00 2d 2d 00 00 c0 00 40 2d 00 00 c2 00 58 2d 00 00 c5 00 60	.....|..*..}..+..~..+.. ...+.....+....(+.....+....=+.. ..N+....W+....l+....y+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..h,.....,.....,.....,.....-.....-....".-....)-....,-....--....@-....X-....`	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\en-GB.pak	unknown	72141	05 00 00 00 01 00 00 00 b0 06 b7 00 7c 00 0e 2b 00 00 7d 00 1d 2b 00 00 7e 00 28 2b 00 00 80 00 30 2b 00 00 81 00 35 2b 00 00 82 00 42 2b 00 00 83 00 48 2b 00 00 84 00 57 2b 00 00 85 00 68 2b 00 00 86 00 71 2b 00 00 88 00 86 2b 00 00 89 00 93 2b 00 00 8b 00 99 2b 00 00 8c 00 a8 2b 00 00 8e 00 ae 2b 00 00 8f 00 c0 2b 00 00 91 00 c8 2b 00 00 92 00 cd 2b 00 00 94 00 d5 2b 00 00 9d 00 dd 2b 00 00 9e 00 e5 2b 00 00 9f 00 ec 2b 00 00 a0 00 f3 2b 00 00 a3 00 fa 2b 00 00 a4 00 fb 2b 00 00 a6 00 fc 2b 00 00 a7 00 09 2c 00 00 a8 00 18 2c 00 00 b1 00 28 2c 00 00 b4 00 37 2c 00 00 b5 00 48 2c 00 00 b6 00 50 2c 00 00 b7 00 58 2c 00 00 b8 00 5f 2c 00 00 bc 00 64 2c 00 00 bd 00 6b 2c 00 00 be 00 6e 2c 00 00 bf 00 6f 2c 00 00 c0 00 74 2c 00 00 c2 00 7f 2c 00 00 c5 00 83	.....|..+..}..+..~.(+.. ..0+....5+....B+....H+....W+.. ..h+....q+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.... (,....7,....H,....P,.....X,.. .._,....d,....k,....n,....o,.. ..t,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\en-US.pak	unknown	72950	05 00 00 00 01 00 00 00 b7 06 b0 00 7c 00 1c 2b 00 00 7d 00 2b 2b 00 00 7e 00 36 2b 00 00 80 00 3e 2b 00 00 81 00 43 2b 00 00 82 00 50 2b 00 00 83 00 56 2b 00 00 84 00 65 2b 00 00 85 00 76 2b 00 00 86 00 7f 2b 00 00 88 00 94 2b 00 00 89 00 a1 2b 00 00 8b 00 a7 2b 00 00 8c 00 b6 2b 00 00 8e 00 bc 2b 00 00 8f 00 ce 2b 00 00 91 00 d6 2b 00 00 92 00 db 2b 00 00 94 00 e3 2b 00 00 9d 00 eb 2b 00 00 9e 00 f3 2b 00 00 9f 00 fa 2b 00 00 a0 00 01 2c 00 00 a3 00 08 2c 00 00 a4 00 09 2c 00 00 a6 00 0a 2c 00 00 a7 00 17 2c 00 00 a8 00 26 2c 00 00 b1 00 36 2c 00 00 b4 00 45 2c 00 00 b5 00 56 2c 00 00 b6 00 5e 2c 00 00 b7 00 66 2c 00 00 b8 00 6d 2c 00 00 bc 00 72 2c 00 00 bd 00 79 2c 00 00 be 00 7c 2c 00 00 bf 00 7d 2c 00 00 c0 00 82 2c 00 00 c2 00 8d 2c 00 00 c5 00 91	.....|..+..}.++..~.6+.. ..>+....C+....P+....V+....e+.. ..v+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,.....,.....,.....,....&,.. ..6,....E,....V,....^,....f,.. ..m,....r,....y,....|,....},.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\es-419.pak	unknown	85292	05 00 00 00 01 00 00 00 af 06 b8 00 7c 00 0c 2b 00 00 7d 00 1b 2b 00 00 7e 00 26 2b 00 00 80 00 2e 2b 00 00 81 00 33 2b 00 00 82 00 40 2b 00 00 83 00 46 2b 00 00 84 00 55 2b 00 00 85 00 66 2b 00 00 86 00 6f 2b 00 00 88 00 84 2b 00 00 89 00 91 2b 00 00 8b 00 97 2b 00 00 8c 00 a6 2b 00 00 8e 00 ac 2b 00 00 8f 00 be 2b 00 00 91 00 c6 2b 00 00 92 00 cb 2b 00 00 94 00 d3 2b 00 00 9d 00 db 2b 00 00 9e 00 e3 2b 00 00 9f 00 ea 2b 00 00 a0 00 f1 2b 00 00 a3 00 f8 2b 00 00 a4 00 f9 2b 00 00 a6 00 fa 2b 00 00 a7 00 0c 2c 00 00 a8 00 1b 2c 00 00 b1 00 30 2c 00 00 b4 00 4a 2c 00 00 b5 00 61 2c 00 00 b6 00 6a 2c 00 00 b7 00 73 2c 00 00 b8 00 7c 2c 00 00 bc 00 82 2c 00 00 bd 00 89 2c 00 00 be 00 8c 2c 00 00 bf 00 8d 2c 00 00 c0 00 94 2c 00 00 c2 00 a5 2c 00 00 c5 00 ab	.....|..+..}..+..~.&+.. ...+....3+....@+....F+....U+.. ..f+....o+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..0,....J,....a,....j,....s,.. ..|,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\es.pak	unknown	86916	05 00 00 00 01 00 00 00 aa 06 bd 00 7c 00 02 2b 00 00 7d 00 11 2b 00 00 7e 00 1c 2b 00 00 80 00 24 2b 00 00 81 00 29 2b 00 00 82 00 36 2b 00 00 83 00 3c 2b 00 00 84 00 4b 2b 00 00 85 00 5c 2b 00 00 86 00 65 2b 00 00 88 00 7a 2b 00 00 89 00 87 2b 00 00 8b 00 8d 2b 00 00 8c 00 9c 2b 00 00 8e 00 a2 2b 00 00 8f 00 b4 2b 00 00 91 00 bc 2b 00 00 92 00 c1 2b 00 00 94 00 c9 2b 00 00 9d 00 d1 2b 00 00 9e 00 d9 2b 00 00 9f 00 e0 2b 00 00 a0 00 e7 2b 00 00 a3 00 ee 2b 00 00 a4 00 ef 2b 00 00 a6 00 f0 2b 00 00 a7 00 03 2c 00 00 a8 00 13 2c 00 00 b1 00 28 2c 00 00 b4 00 42 2c 00 00 b5 00 5a 2c 00 00 b6 00 63 2c 00 00 b7 00 6c 2c 00 00 b8 00 75 2c 00 00 bc 00 7b 2c 00 00 bd 00 82 2c 00 00 be 00 85 2c 00 00 bf 00 86 2c 00 00 c0 00 8d 2c 00 00 c2 00 9e 2c 00 00 c5 00 a4	.....|..+..}..+..~..+.. ..$+....)+....6+....<+....K+.. ..\+....e+....z+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.... (,....B,....Z,....c,....l,....u,.... {,.....,.....,.....,.....,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\et.pak	unknown	77466	05 00 00 00 01 00 00 00 b5 06 b2 00 7c 00 18 2b 00 00 7d 00 27 2b 00 00 7e 00 32 2b 00 00 80 00 3a 2b 00 00 81 00 3f 2b 00 00 82 00 4c 2b 00 00 83 00 52 2b 00 00 84 00 61 2b 00 00 85 00 72 2b 00 00 86 00 7b 2b 00 00 88 00 90 2b 00 00 89 00 9d 2b 00 00 8b 00 a3 2b 00 00 8c 00 b2 2b 00 00 8e 00 b8 2b 00 00 8f 00 ca 2b 00 00 91 00 d2 2b 00 00 92 00 d7 2b 00 00 94 00 df 2b 00 00 9d 00 e7 2b 00 00 9e 00 ef 2b 00 00 9f 00 f6 2b 00 00 a0 00 fd 2b 00 00 a3 00 04 2c 00 00 a4 00 05 2c 00 00 a6 00 06 2c 00 00 a7 00 16 2c 00 00 a8 00 28 2c 00 00 b1 00 3d 2c 00 00 b4 00 4b 2c 00 00 b5 00 61 2c 00 00 b6 00 6a 2c 00 00 b7 00 74 2c 00 00 b8 00 7a 2c 00 00 bc 00 7f 2c 00 00 bd 00 86 2c 00 00 be 00 89 2c 00 00 bf 00 8a 2c 00 00 c0 00 92 2c 00 00 c2 00 9d 2c 00 00 c5 00 a3	.....|..+..}.'+..~.2+.. ..:+....?+....L+....R+....a+.. ..r+....{+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,.....,.....,....(,.. ..=,....K,....a,....j,....t,.. ..z,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\fa.pak	unknown	119827	05 00 00 00 01 00 00 00 96 06 d1 00 7c 00 da 2a 00 00 7d 00 e9 2a 00 00 7e 00 f4 2a 00 00 80 00 fc 2a 00 00 81 00 01 2b 00 00 82 00 0e 2b 00 00 83 00 14 2b 00 00 84 00 23 2b 00 00 85 00 34 2b 00 00 86 00 3d 2b 00 00 88 00 52 2b 00 00 89 00 5f 2b 00 00 8b 00 65 2b 00 00 8c 00 74 2b 00 00 8e 00 7a 2b 00 00 8f 00 8c 2b 00 00 91 00 94 2b 00 00 92 00 99 2b 00 00 94 00 a1 2b 00 00 9d 00 a9 2b 00 00 9e 00 b1 2b 00 00 9f 00 b8 2b 00 00 a0 00 bf 2b 00 00 a3 00 c6 2b 00 00 a6 00 c8 2b 00 00 a7 00 e2 2b 00 00 a8 00 fe 2b 00 00 b1 00 28 2c 00 00 b4 00 48 2c 00 00 b5 00 6f 2c 00 00 b6 00 80 2c 00 00 b7 00 91 2c 00 00 b8 00 9f 2c 00 00 bc 00 a7 2c 00 00 bd 00 ae 2c 00 00 bf 00 b1 2c 00 00 c0 00 b8 2c 00 00 c2 00 cc 2c 00 00 c5 00 d8 2c 00 00 ce 00 eb 2c 00 00 dc 00 02	.....|..*..}..*..~..*.. ...*.....+.....+.....+....#+.. ..4+....=+....R+...._+....e+.. ..t+....z+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+....(,.. ..H,....o,.....,.....,.....,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\fi.pak	unknown	79870	05 00 00 00 01 00 00 00 a0 06 c7 00 7c 00 ee 2a 00 00 7d 00 fd 2a 00 00 7e 00 08 2b 00 00 80 00 10 2b 00 00 81 00 15 2b 00 00 82 00 22 2b 00 00 83 00 28 2b 00 00 84 00 37 2b 00 00 85 00 48 2b 00 00 86 00 51 2b 00 00 88 00 66 2b 00 00 89 00 73 2b 00 00 8b 00 79 2b 00 00 8c 00 88 2b 00 00 8e 00 8e 2b 00 00 8f 00 a0 2b 00 00 91 00 a8 2b 00 00 92 00 ad 2b 00 00 94 00 b5 2b 00 00 9d 00 bd 2b 00 00 9e 00 c5 2b 00 00 9f 00 cc 2b 00 00 a0 00 d3 2b 00 00 a3 00 da 2b 00 00 a4 00 db 2b 00 00 a6 00 dc 2b 00 00 a7 00 ee 2b 00 00 a8 00 ff 2b 00 00 b1 00 12 2c 00 00 b4 00 2b 2c 00 00 b5 00 44 2c 00 00 b6 00 4d 2c 00 00 b7 00 55 2c 00 00 b8 00 5c 2c 00 00 bc 00 61 2c 00 00 bd 00 68 2c 00 00 be 00 6b 2c 00 00 bf 00 6c 2c 00 00 c0 00 73 2c 00 00 c2 00 82 2c 00 00 c5 00 8b	.....|..*..}..*..~..+.. ...+.....+...."+....(+....7+.. ..H+....Q+....f+....s+....y+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,....+,....D,....M,....U,.. ..\,....a,....h,....k,....l,.. ..s,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\fil.pak	unknown	88121	05 00 00 00 01 00 00 00 af 06 b8 00 7c 00 0c 2b 00 00 7d 00 1b 2b 00 00 7e 00 26 2b 00 00 80 00 2e 2b 00 00 81 00 33 2b 00 00 82 00 40 2b 00 00 83 00 46 2b 00 00 84 00 55 2b 00 00 85 00 66 2b 00 00 86 00 6f 2b 00 00 88 00 84 2b 00 00 89 00 91 2b 00 00 8b 00 97 2b 00 00 8c 00 a6 2b 00 00 8e 00 ac 2b 00 00 8f 00 be 2b 00 00 91 00 c6 2b 00 00 92 00 cb 2b 00 00 94 00 d3 2b 00 00 9d 00 db 2b 00 00 9e 00 e3 2b 00 00 9f 00 ea 2b 00 00 a0 00 f1 2b 00 00 a3 00 f8 2b 00 00 a4 00 f9 2b 00 00 a6 00 fa 2b 00 00 a7 00 07 2c 00 00 a8 00 1c 2c 00 00 b1 00 32 2c 00 00 b4 00 45 2c 00 00 b5 00 61 2c 00 00 b6 00 69 2c 00 00 b7 00 71 2c 00 00 b8 00 7c 2c 00 00 bc 00 81 2c 00 00 bd 00 88 2c 00 00 be 00 8b 2c 00 00 bf 00 8c 2c 00 00 c0 00 95 2c 00 00 c2 00 a6 2c 00 00 c5 00 ad	.....|..+..}..+..~.&+.. ...+....3+....@+....F+....U+.. ..f+....o+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..2,....E,....a,....i,....q,.. ..|.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\fr.pak	unknown	93269	05 00 00 00 01 00 00 00 a9 06 be 00 7c 00 00 2b 00 00 7d 00 0f 2b 00 00 7e 00 1a 2b 00 00 80 00 22 2b 00 00 81 00 27 2b 00 00 82 00 34 2b 00 00 83 00 3a 2b 00 00 84 00 49 2b 00 00 85 00 5a 2b 00 00 86 00 63 2b 00 00 88 00 78 2b 00 00 89 00 85 2b 00 00 8b 00 8b 2b 00 00 8c 00 9a 2b 00 00 8e 00 a0 2b 00 00 8f 00 b2 2b 00 00 91 00 ba 2b 00 00 92 00 bf 2b 00 00 94 00 c7 2b 00 00 9d 00 cf 2b 00 00 9e 00 d7 2b 00 00 9f 00 de 2b 00 00 a0 00 e5 2b 00 00 a3 00 ec 2b 00 00 a4 00 ed 2b 00 00 a6 00 ee 2b 00 00 a7 00 fe 2b 00 00 a8 00 0c 2c 00 00 b1 00 1e 2c 00 00 b4 00 35 2c 00 00 b5 00 44 2c 00 00 b6 00 4c 2c 00 00 b7 00 54 2c 00 00 b8 00 5d 2c 00 00 bc 00 63 2c 00 00 bd 00 6a 2c 00 00 be 00 6d 2c 00 00 bf 00 6e 2c 00 00 c0 00 75 2c 00 00 c2 00 88 2c 00 00 c5 00 8e	.....|..+..}..+..~..+.. ..'+....'+....4+....:+....I+.. ..Z+....c+....x+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,....5,....D,....L,....T,.. ..],....c,....j,....m,....n,.. ..u,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\gu.pak	unknown	167056	05 00 00 00 01 00 00 00 a6 06 c1 00 7c 00 fa 2a 00 00 7d 00 09 2b 00 00 7e 00 14 2b 00 00 80 00 1c 2b 00 00 81 00 21 2b 00 00 82 00 2e 2b 00 00 83 00 34 2b 00 00 84 00 43 2b 00 00 85 00 54 2b 00 00 86 00 5d 2b 00 00 88 00 72 2b 00 00 89 00 7f 2b 00 00 8b 00 85 2b 00 00 8c 00 94 2b 00 00 8e 00 9a 2b 00 00 8f 00 ac 2b 00 00 91 00 b4 2b 00 00 92 00 b9 2b 00 00 94 00 c1 2b 00 00 9d 00 c9 2b 00 00 9e 00 d1 2b 00 00 9f 00 d8 2b 00 00 a0 00 df 2b 00 00 a3 00 e6 2b 00 00 a4 00 e7 2b 00 00 a6 00 e8 2b 00 00 a7 00 10 2c 00 00 a8 00 3b 2c 00 00 b1 00 6c 2c 00 00 b4 00 9a 2c 00 00 b5 00 ce 2c 00 00 b6 00 e7 2c 00 00 b7 00 00 2d 00 00 b8 00 2b 2d 00 00 bc 00 3e 2d 00 00 bd 00 45 2d 00 00 be 00 48 2d 00 00 bf 00 4a 2d 00 00 c0 00 61 2d 00 00 c2 00 82 2d 00 00 c5 00 8e	.....|..*..}..+..~..+.. ...+....!+.....+....4+....C+.. ..T+....]+....r+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,....;.. ..I,.....,.....,.....,.....-....+-....>- ....E-....H-....J-....a-.....-.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\he.pak	unknown	104924	05 00 00 00 01 00 00 00 a0 06 c7 00 7c 00 ee 2a 00 00 7d 00 fd 2a 00 00 7e 00 08 2b 00 00 80 00 10 2b 00 00 81 00 15 2b 00 00 82 00 22 2b 00 00 83 00 28 2b 00 00 84 00 37 2b 00 00 85 00 48 2b 00 00 86 00 51 2b 00 00 88 00 66 2b 00 00 89 00 73 2b 00 00 8b 00 79 2b 00 00 8c 00 88 2b 00 00 8e 00 8e 2b 00 00 8f 00 a0 2b 00 00 91 00 a8 2b 00 00 92 00 ad 2b 00 00 94 00 b5 2b 00 00 9d 00 bd 2b 00 00 9e 00 c5 2b 00 00 9f 00 cc 2b 00 00 a0 00 d3 2b 00 00 a3 00 da 2b 00 00 a4 00 db 2b 00 00 a6 00 dc 2b 00 00 a7 00 f3 2b 00 00 a8 00 0c 2c 00 00 b1 00 25 2c 00 00 b4 00 3c 2c 00 00 b5 00 59 2c 00 00 b6 00 61 2c 00 00 b7 00 69 2c 00 00 b8 00 71 2c 00 00 bc 00 79 2c 00 00 bd 00 80 2c 00 00 be 00 83 2c 00 00 bf 00 84 2c 00 00 c0 00 8d 2c 00 00 c2 00 9b 2c 00 00 c5 00 a3	.....|..*..}..*..~..+.. ...+.....+...."+....(+....7+.. ..H+....Q+....f+....s+....y+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ..%,....<,....Y,....a,....i,.. ..q,....y,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\hi.pak	unknown	171191	05 00 00 00 01 00 00 00 99 06 ce 00 7c 00 e0 2a 00 00 7d 00 ef 2a 00 00 7e 00 fa 2a 00 00 80 00 02 2b 00 00 81 00 07 2b 00 00 82 00 14 2b 00 00 83 00 1a 2b 00 00 84 00 29 2b 00 00 85 00 3a 2b 00 00 86 00 43 2b 00 00 88 00 58 2b 00 00 89 00 65 2b 00 00 8b 00 6b 2b 00 00 8c 00 7a 2b 00 00 8e 00 80 2b 00 00 8f 00 92 2b 00 00 91 00 9a 2b 00 00 92 00 9f 2b 00 00 94 00 a7 2b 00 00 9d 00 af 2b 00 00 9e 00 b7 2b 00 00 9f 00 be 2b 00 00 a0 00 c5 2b 00 00 a3 00 cc 2b 00 00 a4 00 cd 2b 00 00 a6 00 ce 2b 00 00 a7 00 f0 2b 00 00 a8 00 15 2c 00 00 b1 00 40 2c 00 00 b4 00 62 2c 00 00 b5 00 93 2c 00 00 b6 00 ac 2c 00 00 b7 00 c5 2c 00 00 b8 00 f6 2c 00 00 bc 00 0c 2d 00 00 bd 00 13 2d 00 00 be 00 16 2d 00 00 bf 00 18 2d 00 00 c0 00 44 2d 00 00 c2 00 65 2d 00 00 c5 00 71	.....|..*..}..*..~..*.. ...+.....+.....+.....+....)+.. ..:+....C+....X+....e+....k+.. ..z+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ..@,....b,.....,.....,.....,.. ...,.....-.....-.....-.....-....D- ....e-....q	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\hr.pak	unknown	84709	05 00 00 00 01 00 00 00 b3 06 b4 00 7c 00 14 2b 00 00 7d 00 23 2b 00 00 7e 00 2e 2b 00 00 80 00 36 2b 00 00 81 00 3b 2b 00 00 82 00 48 2b 00 00 83 00 4e 2b 00 00 84 00 5d 2b 00 00 85 00 6e 2b 00 00 86 00 77 2b 00 00 88 00 8c 2b 00 00 89 00 99 2b 00 00 8b 00 9f 2b 00 00 8c 00 ae 2b 00 00 8e 00 b4 2b 00 00 8f 00 c6 2b 00 00 91 00 ce 2b 00 00 92 00 d3 2b 00 00 94 00 db 2b 00 00 9d 00 e3 2b 00 00 9e 00 eb 2b 00 00 9f 00 f2 2b 00 00 a0 00 f9 2b 00 00 a3 00 00 2c 00 00 a4 00 01 2c 00 00 a6 00 02 2c 00 00 a7 00 0e 2c 00 00 a8 00 1a 2c 00 00 b1 00 28 2c 00 00 b4 00 45 2c 00 00 b5 00 56 2c 00 00 b6 00 61 2c 00 00 b7 00 6d 2c 00 00 b8 00 72 2c 00 00 bc 00 79 2c 00 00 bd 00 80 2c 00 00 be 00 83 2c 00 00 bf 00 84 2c 00 00 c0 00 8c 2c 00 00 c2 00 98 2c 00 00 c5 00 9e	.....|..+..}.#+..~..+.. ..6+....;+....H+....N+....]+.. ..n+....w+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,.....,.....,.....,.... (,....E,....V,....a,....m,.. ..r,....y,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\hu.pak	unknown	89863	05 00 00 00 01 00 00 00 a8 06 bf 00 7c 00 fe 2a 00 00 7d 00 0d 2b 00 00 7e 00 18 2b 00 00 80 00 20 2b 00 00 81 00 25 2b 00 00 82 00 32 2b 00 00 83 00 38 2b 00 00 84 00 47 2b 00 00 85 00 58 2b 00 00 86 00 61 2b 00 00 88 00 76 2b 00 00 89 00 83 2b 00 00 8b 00 89 2b 00 00 8c 00 98 2b 00 00 8e 00 9e 2b 00 00 8f 00 b0 2b 00 00 91 00 b8 2b 00 00 92 00 bd 2b 00 00 94 00 c5 2b 00 00 9d 00 cd 2b 00 00 9e 00 d5 2b 00 00 9f 00 dc 2b 00 00 a0 00 e3 2b 00 00 a3 00 ea 2b 00 00 a4 00 eb 2b 00 00 a6 00 ec 2b 00 00 a7 00 fc 2b 00 00 a8 00 12 2c 00 00 b1 00 27 2c 00 00 b4 00 3c 2c 00 00 b5 00 50 2c 00 00 b6 00 5d 2c 00 00 b7 00 6a 2c 00 00 b8 00 7a 2c 00 00 bc 00 83 2c 00 00 bd 00 8a 2c 00 00 be 00 8d 2c 00 00 bf 00 8e 2c 00 00 c0 00 98 2c 00 00 c2 00 af 2c 00 00 c5 00 b5	.....|..*..}..+..~..+.... +....%+....2+....8+....G+.. ..X+....a+....v+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,....',.... <,....P,....],....j,.. ..z,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\id.pak	unknown	77956	05 00 00 00 01 00 00 00 a0 06 c7 00 7c 00 ee 2a 00 00 7d 00 fd 2a 00 00 7e 00 08 2b 00 00 80 00 10 2b 00 00 81 00 15 2b 00 00 82 00 22 2b 00 00 83 00 28 2b 00 00 84 00 37 2b 00 00 85 00 48 2b 00 00 86 00 51 2b 00 00 88 00 66 2b 00 00 89 00 73 2b 00 00 8b 00 79 2b 00 00 8c 00 88 2b 00 00 8e 00 8e 2b 00 00 8f 00 a0 2b 00 00 91 00 a8 2b 00 00 92 00 ad 2b 00 00 94 00 b5 2b 00 00 9d 00 bd 2b 00 00 9e 00 c5 2b 00 00 9f 00 cc 2b 00 00 a0 00 d3 2b 00 00 a3 00 da 2b 00 00 a4 00 db 2b 00 00 a6 00 dc 2b 00 00 a7 00 ea 2b 00 00 a8 00 f7 2b 00 00 b1 00 07 2c 00 00 b4 00 18 2c 00 00 b5 00 2a 2c 00 00 b6 00 32 2c 00 00 b7 00 3a 2c 00 00 b8 00 42 2c 00 00 bc 00 47 2c 00 00 bd 00 4e 2c 00 00 be 00 51 2c 00 00 bf 00 52 2c 00 00 c0 00 58 2c 00 00 c2 00 64 2c 00 00 c5 00 6a	.....|..*..}..*..~..+.. ...+.....+...."+....(+....7+.. ..H+....Q+....f+....s+....y+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,....*,....2,....:,.. ..B,....G,....N,....Q,....R,.. ..X,....d,....j	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\it.pak	unknown	84595	05 00 00 00 01 00 00 00 ad 06 ba 00 7c 00 08 2b 00 00 7d 00 17 2b 00 00 7e 00 22 2b 00 00 80 00 2a 2b 00 00 81 00 2f 2b 00 00 82 00 3c 2b 00 00 83 00 42 2b 00 00 84 00 51 2b 00 00 85 00 62 2b 00 00 86 00 6b 2b 00 00 88 00 80 2b 00 00 89 00 8d 2b 00 00 8b 00 93 2b 00 00 8c 00 a2 2b 00 00 8e 00 a8 2b 00 00 8f 00 ba 2b 00 00 91 00 c2 2b 00 00 92 00 c7 2b 00 00 94 00 cf 2b 00 00 9d 00 d7 2b 00 00 9e 00 df 2b 00 00 9f 00 e6 2b 00 00 a0 00 ed 2b 00 00 a3 00 f4 2b 00 00 a4 00 f5 2b 00 00 a6 00 f6 2b 00 00 a7 00 09 2c 00 00 a8 00 18 2c 00 00 b1 00 31 2c 00 00 b4 00 36 2c 00 00 b5 00 47 2c 00 00 b6 00 55 2c 00 00 b7 00 60 2c 00 00 b8 00 6a 2c 00 00 bc 00 70 2c 00 00 bd 00 77 2c 00 00 be 00 7a 2c 00 00 bf 00 7b 2c 00 00 c0 00 81 2c 00 00 c2 00 91 2c 00 00 c5 00 99	.....|..+..}..+..~."+.. ..*+..../+....<+....B+....Q+.. ..b+....k+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..1,....6,....G,....U,....`,.. ..j,....p,....w,....z,....{,... ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\ja.pak	unknown	102149	05 00 00 00 01 00 00 00 7e 06 e9 00 7c 00 aa 2a 00 00 7d 00 bb 2a 00 00 7e 00 c4 2a 00 00 7f 00 cc 2a 00 00 81 00 e1 2a 00 00 82 00 ee 2a 00 00 83 00 f4 2a 00 00 88 00 03 2b 00 00 89 00 10 2b 00 00 8b 00 16 2b 00 00 8c 00 25 2b 00 00 8e 00 2b 2b 00 00 8f 00 3d 2b 00 00 91 00 45 2b 00 00 92 00 4a 2b 00 00 93 00 52 2b 00 00 94 00 5d 2b 00 00 95 00 65 2b 00 00 98 00 74 2b 00 00 9d 00 79 2b 00 00 9e 00 81 2b 00 00 9f 00 88 2b 00 00 a0 00 8f 2b 00 00 a3 00 96 2b 00 00 a6 00 98 2b 00 00 a7 00 b1 2b 00 00 a8 00 cf 2b 00 00 b1 00 f0 2b 00 00 b4 00 ff 2b 00 00 b5 00 20 2c 00 00 b6 00 29 2c 00 00 b7 00 32 2c 00 00 b8 00 38 2c 00 00 bc 00 41 2c 00 00 bd 00 48 2c 00 00 bf 00 4b 2c 00 00 c0 00 58 2c 00 00 c2 00 6b 2c 00 00 c5 00 71 2c 00 00 ce 00 77 2c 00 00 dc 00 7d	.....~...|..*..}..*..~..*.. ...*.....*.....*.....*.....+.. ...+.....+....%+....++....=+.. ..E+....J+....R+....]+....e+.. ..t+....y+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.... ,....),....2,....8,.. ..A,....H,....K,....X,....k,.. ..q,....w,....}	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\kn.pak	unknown	191849	05 00 00 00 01 00 00 00 ab 06 bc 00 7c 00 04 2b 00 00 7d 00 13 2b 00 00 7e 00 1e 2b 00 00 80 00 26 2b 00 00 81 00 2b 2b 00 00 82 00 38 2b 00 00 83 00 3e 2b 00 00 84 00 4d 2b 00 00 85 00 5e 2b 00 00 86 00 67 2b 00 00 88 00 7c 2b 00 00 89 00 89 2b 00 00 8b 00 8f 2b 00 00 8c 00 9e 2b 00 00 8e 00 a4 2b 00 00 8f 00 b6 2b 00 00 91 00 be 2b 00 00 92 00 c3 2b 00 00 94 00 cb 2b 00 00 9d 00 d3 2b 00 00 9e 00 db 2b 00 00 9f 00 e2 2b 00 00 a0 00 e9 2b 00 00 a3 00 f0 2b 00 00 a4 00 f1 2b 00 00 a6 00 f2 2b 00 00 a7 00 29 2c 00 00 a8 00 60 2c 00 00 b1 00 a0 2c 00 00 b4 00 c8 2c 00 00 b5 00 14 2d 00 00 b6 00 2c 2d 00 00 b7 00 50 2d 00 00 b8 00 6e 2d 00 00 bc 00 86 2d 00 00 bd 00 8d 2d 00 00 be 00 90 2d 00 00 bf 00 92 2d 00 00 c0 00 a5 2d 00 00 c2 00 cf 2d 00 00 c5 00 de	.....|..+..}..+..~..+.. ..&+....++....8+....>+....M+.. ..^+....g+....|+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+....),....`,.. ...,.....,.....-....,-....P-....n-.....-.....-.....-.....-.....-.....-.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\ko.pak	unknown	86324	05 00 00 00 01 00 00 00 83 06 e4 00 7c 00 b4 2a 00 00 7d 00 c1 2a 00 00 7e 00 c9 2a 00 00 7f 00 d1 2a 00 00 81 00 d7 2a 00 00 82 00 de 2a 00 00 83 00 e4 2a 00 00 84 00 f3 2a 00 00 85 00 04 2b 00 00 86 00 0d 2b 00 00 8b 00 22 2b 00 00 8c 00 31 2b 00 00 8e 00 37 2b 00 00 8f 00 49 2b 00 00 91 00 51 2b 00 00 92 00 56 2b 00 00 93 00 5e 2b 00 00 94 00 69 2b 00 00 95 00 71 2b 00 00 98 00 80 2b 00 00 9f 00 85 2b 00 00 a0 00 8c 2b 00 00 a3 00 93 2b 00 00 a6 00 95 2b 00 00 a7 00 a1 2b 00 00 a8 00 b1 2b 00 00 b1 00 c4 2b 00 00 b4 00 d4 2b 00 00 b5 00 e4 2b 00 00 b6 00 ed 2b 00 00 b7 00 f6 2b 00 00 b8 00 fc 2b 00 00 bc 00 02 2c 00 00 bd 00 09 2c 00 00 bf 00 0c 2c 00 00 c0 00 16 2c 00 00 c2 00 27 2c 00 00 c5 00 2d 2c 00 00 ce 00 36 2c 00 00 dc 00 4c 2c 00 00 dd 00 5e	.....|..*..}..*..~..*.. ...*.....*.....*.....*.....*.. ...+.....+....".+....1+....7+.. ..I+....Q+....V+....^+....i+.. ..q+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,.....,.....,....',....-,.. ..6,....L,....^	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\lt.pak	unknown	91387	05 00 00 00 01 00 00 00 aa 06 bd 00 7c 00 02 2b 00 00 7d 00 11 2b 00 00 7e 00 1c 2b 00 00 80 00 24 2b 00 00 81 00 29 2b 00 00 82 00 36 2b 00 00 83 00 3c 2b 00 00 84 00 4b 2b 00 00 85 00 5c 2b 00 00 86 00 65 2b 00 00 88 00 7a 2b 00 00 89 00 87 2b 00 00 8b 00 8d 2b 00 00 8c 00 9c 2b 00 00 8e 00 a2 2b 00 00 8f 00 b4 2b 00 00 91 00 bc 2b 00 00 92 00 c1 2b 00 00 94 00 c9 2b 00 00 9d 00 d1 2b 00 00 9e 00 d9 2b 00 00 9f 00 e0 2b 00 00 a0 00 e7 2b 00 00 a3 00 ee 2b 00 00 a4 00 ef 2b 00 00 a6 00 f0 2b 00 00 a7 00 fe 2b 00 00 a8 00 0b 2c 00 00 b1 00 1f 2c 00 00 b4 00 37 2c 00 00 b5 00 48 2c 00 00 b6 00 52 2c 00 00 b7 00 5d 2c 00 00 b8 00 64 2c 00 00 bc 00 6d 2c 00 00 bd 00 74 2c 00 00 be 00 77 2c 00 00 bf 00 78 2c 00 00 c0 00 82 2c 00 00 c2 00 94 2c 00 00 c5 00 99	.....|..+..}..+..~..+.. ..$+....)+....6+....<+....K+.. ..\+....e+....z+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,....7,....H,....R,....],.. ..d,....m,....t,....w,....x,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\lv.pak	unknown	90503	05 00 00 00 01 00 00 00 b4 06 b3 00 7c 00 16 2b 00 00 7d 00 25 2b 00 00 7e 00 30 2b 00 00 80 00 38 2b 00 00 81 00 3d 2b 00 00 82 00 4a 2b 00 00 83 00 50 2b 00 00 84 00 5f 2b 00 00 85 00 70 2b 00 00 86 00 79 2b 00 00 88 00 8e 2b 00 00 89 00 9b 2b 00 00 8b 00 a1 2b 00 00 8c 00 b0 2b 00 00 8e 00 b6 2b 00 00 8f 00 c8 2b 00 00 91 00 d0 2b 00 00 92 00 d5 2b 00 00 94 00 dd 2b 00 00 9d 00 e5 2b 00 00 9e 00 ed 2b 00 00 9f 00 f4 2b 00 00 a0 00 fb 2b 00 00 a3 00 02 2c 00 00 a4 00 03 2c 00 00 a6 00 04 2c 00 00 a7 00 17 2c 00 00 a8 00 2a 2c 00 00 b1 00 40 2c 00 00 b4 00 5b 2c 00 00 b5 00 77 2c 00 00 b6 00 81 2c 00 00 b7 00 8c 2c 00 00 b8 00 94 2c 00 00 bc 00 9c 2c 00 00 bd 00 a3 2c 00 00 be 00 a6 2c 00 00 bf 00 a7 2c 00 00 c0 00 ae 2c 00 00 c2 00 c0 2c 00 00 c5 00 c8	.....|..+..}.%+..~.0+.. ..8+....=+....J+....P+...._+.. ..p+....y+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,.....,.....,....*,....@,.... [,....w,.....,.....,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\ml.pak	unknown	203423	05 00 00 00 01 00 00 00 a9 06 be 00 7c 00 00 2b 00 00 7d 00 0f 2b 00 00 7e 00 1a 2b 00 00 80 00 22 2b 00 00 81 00 27 2b 00 00 82 00 34 2b 00 00 83 00 3a 2b 00 00 84 00 49 2b 00 00 85 00 5a 2b 00 00 86 00 63 2b 00 00 88 00 78 2b 00 00 89 00 85 2b 00 00 8b 00 8b 2b 00 00 8c 00 9a 2b 00 00 8e 00 a0 2b 00 00 8f 00 b2 2b 00 00 91 00 ba 2b 00 00 92 00 bf 2b 00 00 94 00 c7 2b 00 00 9d 00 cf 2b 00 00 9e 00 d7 2b 00 00 9f 00 de 2b 00 00 a0 00 e5 2b 00 00 a3 00 ec 2b 00 00 a4 00 ed 2b 00 00 a6 00 ee 2b 00 00 a7 00 25 2c 00 00 a8 00 6b 2c 00 00 b1 00 ab 2c 00 00 b4 00 d3 2c 00 00 b5 00 1f 2d 00 00 b6 00 43 2d 00 00 b7 00 61 2d 00 00 b8 00 8e 2d 00 00 bc 00 a9 2d 00 00 bd 00 b0 2d 00 00 be 00 b3 2d 00 00 bf 00 b5 2d 00 00 c0 00 d1 2d 00 00 c2 00 0c 2e 00 00 c5 00 2a	.....|..+..}..+..~..+.. .."+....'+....4+....:+....I+.. ..Z+....c+....x+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+....%,....k,.. ...,.....,.....-....C-....a-.....-.....-.....-.....-.....-.....-.....-.....*	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\mr.pak	unknown	165740	05 00 00 00 01 00 00 00 a0 06 c7 00 7c 00 ee 2a 00 00 7d 00 fd 2a 00 00 7e 00 08 2b 00 00 80 00 10 2b 00 00 81 00 15 2b 00 00 82 00 22 2b 00 00 83 00 28 2b 00 00 84 00 37 2b 00 00 85 00 48 2b 00 00 86 00 51 2b 00 00 88 00 66 2b 00 00 89 00 73 2b 00 00 8b 00 79 2b 00 00 8c 00 88 2b 00 00 8e 00 8e 2b 00 00 8f 00 a0 2b 00 00 91 00 a8 2b 00 00 92 00 ad 2b 00 00 94 00 b5 2b 00 00 9d 00 bd 2b 00 00 9e 00 c5 2b 00 00 9f 00 cc 2b 00 00 a0 00 d3 2b 00 00 a3 00 da 2b 00 00 a4 00 db 2b 00 00 a6 00 dc 2b 00 00 a7 00 fe 2b 00 00 a8 00 20 2c 00 00 b1 00 3f 2c 00 00 b4 00 67 2c 00 00 b5 00 b4 2c 00 00 b6 00 ca 2c 00 00 b7 00 d9 2c 00 00 b8 00 04 2d 00 00 bc 00 17 2d 00 00 bd 00 1e 2d 00 00 be 00 21 2d 00 00 bf 00 23 2d 00 00 c0 00 3a 2d 00 00 c2 00 57 2d 00 00 c5 00 66	.....|..*..}..*..~..+.. ...+.....+....".+....(+....7+.. ..H+....Q+....f+....s+....y+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.... ,.. ..?,....g,.....,.....,.....,.....-.....-.....-....l-....#-....:-....W-....f	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\ms.pak	unknown	79456	05 00 00 00 01 00 00 00 a4 06 c3 00 7c 00 f6 2a 00 00 7d 00 05 2b 00 00 7e 00 10 2b 00 00 80 00 18 2b 00 00 81 00 1d 2b 00 00 82 00 2a 2b 00 00 83 00 30 2b 00 00 84 00 3f 2b 00 00 85 00 50 2b 00 00 86 00 59 2b 00 00 88 00 6e 2b 00 00 89 00 7b 2b 00 00 8b 00 81 2b 00 00 8c 00 90 2b 00 00 8e 00 96 2b 00 00 8f 00 a8 2b 00 00 91 00 b0 2b 00 00 92 00 b5 2b 00 00 94 00 bd 2b 00 00 9d 00 c5 2b 00 00 9e 00 cd 2b 00 00 9f 00 d4 2b 00 00 a0 00 db 2b 00 00 a3 00 e2 2b 00 00 a4 00 e3 2b 00 00 a6 00 e4 2b 00 00 a7 00 f7 2b 00 00 a8 00 0b 2c 00 00 b1 00 25 2c 00 00 b4 00 32 2c 00 00 b5 00 49 2c 00 00 b6 00 53 2c 00 00 b7 00 5e 2c 00 00 b8 00 66 2c 00 00 bc 00 6b 2c 00 00 bd 00 72 2c 00 00 be 00 75 2c 00 00 bf 00 76 2c 00 00 c0 00 7c 2c 00 00 c2 00 88 2c 00 00 c5 00 8f	.....|..*..}..+..~..+.. ...+.....+....*+....0+....?+.. ..P+....Y+....n+....{+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ..%,....2,....I,....S,....^,.. ..f,....k,....r,....u,....v,.. ..|,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\nb.pak	unknown	78385	05 00 00 00 01 00 00 00 a6 06 c1 00 7c 00 fa 2a 00 00 7d 00 09 2b 00 00 7e 00 14 2b 00 00 80 00 1c 2b 00 00 81 00 21 2b 00 00 82 00 2e 2b 00 00 83 00 34 2b 00 00 84 00 43 2b 00 00 85 00 54 2b 00 00 86 00 5d 2b 00 00 88 00 72 2b 00 00 89 00 7f 2b 00 00 8b 00 85 2b 00 00 8c 00 94 2b 00 00 8e 00 9a 2b 00 00 8f 00 ac 2b 00 00 91 00 b4 2b 00 00 92 00 b9 2b 00 00 94 00 c1 2b 00 00 9d 00 c9 2b 00 00 9e 00 d1 2b 00 00 9f 00 d8 2b 00 00 a0 00 df 2b 00 00 a3 00 e6 2b 00 00 a4 00 e7 2b 00 00 a6 00 e8 2b 00 00 a7 00 f3 2b 00 00 a8 00 02 2c 00 00 b1 00 15 2c 00 00 b4 00 24 2c 00 00 b5 00 3b 2c 00 00 b6 00 42 2c 00 00 b7 00 4a 2c 00 00 b8 00 55 2c 00 00 bc 00 59 2c 00 00 bd 00 60 2c 00 00 be 00 63 2c 00 00 bf 00 64 2c 00 00 c0 00 6b 2c 00 00 c2 00 76 2c 00 00 c5 00 7d	.....|..*..}..+..~..+.. ...+....!+.....+....4+....C+.. ..T+....]+....r+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,....$,....;,....B,.....J,.. ..U,....Y,....`,....c,....d,.. ..k,....v,....}	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\nl.pak	unknown	82287	05 00 00 00 01 00 00 00 ad 06 ba 00 7c 00 08 2b 00 00 7d 00 17 2b 00 00 7e 00 22 2b 00 00 80 00 2a 2b 00 00 81 00 2f 2b 00 00 82 00 3c 2b 00 00 83 00 42 2b 00 00 84 00 51 2b 00 00 85 00 62 2b 00 00 86 00 6b 2b 00 00 88 00 80 2b 00 00 89 00 8d 2b 00 00 8b 00 93 2b 00 00 8c 00 a2 2b 00 00 8e 00 a8 2b 00 00 8f 00 ba 2b 00 00 91 00 c2 2b 00 00 92 00 c7 2b 00 00 94 00 cf 2b 00 00 9d 00 d7 2b 00 00 9e 00 df 2b 00 00 9f 00 e6 2b 00 00 a0 00 ed 2b 00 00 a3 00 f4 2b 00 00 a4 00 f5 2b 00 00 a6 00 f6 2b 00 00 a7 00 04 2c 00 00 a8 00 16 2c 00 00 b1 00 29 2c 00 00 b4 00 3b 2c 00 00 b5 00 4f 2c 00 00 b6 00 5c 2c 00 00 b7 00 69 2c 00 00 b8 00 73 2c 00 00 bc 00 7a 2c 00 00 bd 00 81 2c 00 00 be 00 84 2c 00 00 bf 00 85 2c 00 00 c0 00 8f 2c 00 00 c2 00 a0 2c 00 00 c5 00 a6	.....|..+..}..+..~."+.. ..*+..../+....<+....B+....Q+.. ..b+....k+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..),....;,....O,....\,....i,.. ..s,....z,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\pl.pak	unknown	88465	05 00 00 00 01 00 00 00 ae 06 b9 00 7c 00 0a 2b 00 00 7d 00 19 2b 00 00 7e 00 24 2b 00 00 80 00 2c 2b 00 00 81 00 31 2b 00 00 82 00 3e 2b 00 00 83 00 44 2b 00 00 84 00 53 2b 00 00 85 00 64 2b 00 00 86 00 6d 2b 00 00 88 00 82 2b 00 00 89 00 8f 2b 00 00 8b 00 95 2b 00 00 8c 00 a4 2b 00 00 8e 00 aa 2b 00 00 8f 00 bc 2b 00 00 91 00 c4 2b 00 00 92 00 c9 2b 00 00 94 00 d1 2b 00 00 9d 00 d9 2b 00 00 9e 00 e1 2b 00 00 9f 00 e8 2b 00 00 a0 00 ef 2b 00 00 a3 00 f6 2b 00 00 a4 00 f7 2b 00 00 a6 00 f8 2b 00 00 a7 00 07 2c 00 00 a8 00 15 2c 00 00 b1 00 2a 2c 00 00 b4 00 2f 2c 00 00 b5 00 44 2c 00 00 b6 00 4f 2c 00 00 b7 00 5b 2c 00 00 b8 00 65 2c 00 00 bc 00 6c 2c 00 00 bd 00 73 2c 00 00 be 00 76 2c 00 00 bf 00 77 2c 00 00 c0 00 7e 2c 00 00 c2 00 8f 2c 00 00 c5 00 95	.....|..+..}..+..~.$+.. ..,+....1+....>+....D+....S+.. ..d+....m+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..*,..../,....D,....O,....[,.. ..e,....l,....s,....v,....w,.. ..~,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\pt-BR.pak	unknown	84446	05 00 00 00 01 00 00 00 ab 06 bc 00 7c 00 04 2b 00 00 7d 00 13 2b 00 00 7e 00 1e 2b 00 00 80 00 26 2b 00 00 81 00 2b 2b 00 00 82 00 38 2b 00 00 83 00 3e 2b 00 00 84 00 4d 2b 00 00 85 00 5e 2b 00 00 86 00 67 2b 00 00 88 00 7c 2b 00 00 89 00 89 2b 00 00 8b 00 8f 2b 00 00 8c 00 9e 2b 00 00 8e 00 a4 2b 00 00 8f 00 b6 2b 00 00 91 00 be 2b 00 00 92 00 c3 2b 00 00 94 00 cb 2b 00 00 9d 00 d3 2b 00 00 9e 00 db 2b 00 00 9f 00 e2 2b 00 00 a0 00 e9 2b 00 00 a3 00 f0 2b 00 00 a4 00 f1 2b 00 00 a6 00 f2 2b 00 00 a7 00 04 2c 00 00 a8 00 14 2c 00 00 b1 00 35 2c 00 00 b4 00 4d 2c 00 00 b5 00 62 2c 00 00 b6 00 6b 2c 00 00 b7 00 74 2c 00 00 b8 00 7d 2c 00 00 bc 00 83 2c 00 00 bd 00 8a 2c 00 00 be 00 8d 2c 00 00 bf 00 8e 2c 00 00 c0 00 95 2c 00 00 c2 00 a5 2c 00 00 c5 00 ab	.....|..+..}..+..~..+.. ..&+....++....8+....>+....M+.. ..^+....g+....|+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..5,....M,....b,....k,....t,.. ..},.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\pt-PT.pak	unknown	84703	05 00 00 00 01 00 00 00 b1 06 b6 00 7c 00 10 2b 00 00 7d 00 1f 2b 00 00 7e 00 2a 2b 00 00 80 00 32 2b 00 00 81 00 37 2b 00 00 82 00 44 2b 00 00 83 00 4a 2b 00 00 84 00 59 2b 00 00 85 00 6a 2b 00 00 86 00 73 2b 00 00 88 00 88 2b 00 00 89 00 95 2b 00 00 8b 00 9b 2b 00 00 8c 00 aa 2b 00 00 8e 00 b0 2b 00 00 8f 00 c2 2b 00 00 91 00 ca 2b 00 00 92 00 cf 2b 00 00 94 00 d7 2b 00 00 9d 00 df 2b 00 00 9e 00 e7 2b 00 00 9f 00 ee 2b 00 00 a0 00 f5 2b 00 00 a3 00 fc 2b 00 00 a4 00 fd 2b 00 00 a6 00 fe 2b 00 00 a7 00 11 2c 00 00 a8 00 22 2c 00 00 b1 00 37 2c 00 00 b4 00 52 2c 00 00 b5 00 64 2c 00 00 b6 00 6d 2c 00 00 b7 00 76 2c 00 00 b8 00 7f 2c 00 00 bc 00 85 2c 00 00 bd 00 8c 2c 00 00 be 00 8f 2c 00 00 bf 00 90 2c 00 00 c0 00 97 2c 00 00 c2 00 a8 2c 00 00 c5 00 b0	.....|..+..}..+..~.*+.. ..2+....7+....D+....J+....Y+.. ..j+....s+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,....",.. ..7,....R,....d,....m,....v,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\ro.pak	unknown	87484	05 00 00 00 01 00 00 00 b4 06 b3 00 7c 00 16 2b 00 00 7d 00 25 2b 00 00 7e 00 30 2b 00 00 80 00 38 2b 00 00 81 00 3d 2b 00 00 82 00 4a 2b 00 00 83 00 50 2b 00 00 84 00 5f 2b 00 00 85 00 70 2b 00 00 86 00 79 2b 00 00 88 00 8e 2b 00 00 89 00 9b 2b 00 00 8b 00 a1 2b 00 00 8c 00 b0 2b 00 00 8e 00 b6 2b 00 00 8f 00 c8 2b 00 00 91 00 d0 2b 00 00 92 00 d5 2b 00 00 94 00 dd 2b 00 00 9d 00 e5 2b 00 00 9e 00 ed 2b 00 00 9f 00 f4 2b 00 00 a0 00 fb 2b 00 00 a3 00 02 2c 00 00 a4 00 03 2c 00 00 a6 00 04 2c 00 00 a7 00 13 2c 00 00 a8 00 1f 2c 00 00 b1 00 2d 2c 00 00 b4 00 43 2c 00 00 b5 00 55 2c 00 00 b6 00 61 2c 00 00 b7 00 6d 2c 00 00 b8 00 7a 2c 00 00 bc 00 82 2c 00 00 bd 00 89 2c 00 00 be 00 8c 2c 00 00 bf 00 8d 2c 00 00 c0 00 96 2c 00 00 c2 00 a6 2c 00 00 c5 00 ad	.....|..+..}.%+..~.0+.. ..8+....=+....J+....P+...._+.. ..p+....y+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,.....,.....,.....,....- ,....C,....U,....a,....m,.. ..z,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\ru.pak	unknown	134331	05 00 00 00 01 00 00 00 90 06 d7 00 7c 00 ce 2a 00 00 7d 00 dd 2a 00 00 7e 00 e8 2a 00 00 80 00 f0 2a 00 00 81 00 f5 2a 00 00 82 00 02 2b 00 00 83 00 08 2b 00 00 84 00 17 2b 00 00 85 00 28 2b 00 00 86 00 31 2b 00 00 88 00 46 2b 00 00 89 00 53 2b 00 00 8b 00 59 2b 00 00 8c 00 68 2b 00 00 8e 00 6e 2b 00 00 8f 00 80 2b 00 00 91 00 88 2b 00 00 92 00 8d 2b 00 00 94 00 95 2b 00 00 9d 00 9d 2b 00 00 9e 00 a5 2b 00 00 9f 00 ac 2b 00 00 a0 00 b3 2b 00 00 a3 00 ba 2b 00 00 a4 00 bb 2b 00 00 a6 00 bc 2b 00 00 a7 00 d9 2b 00 00 a8 00 f6 2b 00 00 b1 00 0e 2c 00 00 b4 00 3c 2c 00 00 b5 00 63 2c 00 00 b6 00 73 2c 00 00 b7 00 87 2c 00 00 b8 00 9f 2c 00 00 bc 00 ad 2c 00 00 bd 00 b4 2c 00 00 be 00 b7 2c 00 00 bf 00 b8 2c 00 00 c0 00 cd 2c 00 00 c2 00 e5 2c 00 00 c5 00 ef	.....|..*..}..*..~..*.. ...*.....*.....+.....+.....+.... (+....1+....F+....S+....Y+.. ..h+....n+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,....<,....c,....s,.....,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\sk.pak	unknown	89621	05 00 00 00 01 00 00 00 b4 06 b3 00 7c 00 16 2b 00 00 7d 00 25 2b 00 00 7e 00 30 2b 00 00 80 00 38 2b 00 00 81 00 3d 2b 00 00 82 00 4a 2b 00 00 83 00 50 2b 00 00 84 00 5f 2b 00 00 85 00 70 2b 00 00 86 00 79 2b 00 00 88 00 8e 2b 00 00 89 00 9b 2b 00 00 8b 00 a1 2b 00 00 8c 00 b0 2b 00 00 8e 00 b6 2b 00 00 8f 00 c8 2b 00 00 91 00 d0 2b 00 00 92 00 d5 2b 00 00 94 00 dd 2b 00 00 9d 00 e5 2b 00 00 9e 00 ed 2b 00 00 9f 00 f4 2b 00 00 a0 00 fb 2b 00 00 a3 00 02 2c 00 00 a4 00 03 2c 00 00 a6 00 04 2c 00 00 a7 00 18 2c 00 00 a8 00 20 2c 00 00 b1 00 32 2c 00 00 b4 00 4c 2c 00 00 b5 00 61 2c 00 00 b6 00 6f 2c 00 00 b7 00 7d 2c 00 00 b8 00 85 2c 00 00 bc 00 8d 2c 00 00 bd 00 94 2c 00 00 be 00 97 2c 00 00 bf 00 98 2c 00 00 c0 00 a4 2c 00 00 c2 00 b4 2c 00 00 c5 00 bc	.....|..+..}.%+..~.0+.. ..8+....=+....J+....P+...._+.. ..p+....y+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,.....,.....,..... ,.. ..2,....L,....a,....o,....},.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\sl.pak	unknown	85805	05 00 00 00 01 00 00 00 a1 06 c6 00 7c 00 f0 2a 00 00 7d 00 ff 2a 00 00 7e 00 0a 2b 00 00 80 00 12 2b 00 00 81 00 17 2b 00 00 82 00 24 2b 00 00 83 00 2a 2b 00 00 84 00 39 2b 00 00 85 00 4a 2b 00 00 86 00 53 2b 00 00 88 00 68 2b 00 00 89 00 75 2b 00 00 8b 00 7b 2b 00 00 8c 00 8a 2b 00 00 8e 00 90 2b 00 00 8f 00 a2 2b 00 00 91 00 aa 2b 00 00 92 00 af 2b 00 00 94 00 b7 2b 00 00 9d 00 bf 2b 00 00 9e 00 c7 2b 00 00 9f 00 ce 2b 00 00 a0 00 d5 2b 00 00 a3 00 dc 2b 00 00 a4 00 dd 2b 00 00 a6 00 de 2b 00 00 a7 00 f0 2b 00 00 a8 00 fe 2b 00 00 b1 00 0e 2c 00 00 b4 00 26 2c 00 00 b5 00 39 2c 00 00 b6 00 43 2c 00 00 b7 00 4b 2c 00 00 b8 00 51 2c 00 00 bc 00 56 2c 00 00 bd 00 5d 2c 00 00 be 00 60 2c 00 00 bf 00 61 2c 00 00 c0 00 69 2c 00 00 c2 00 74 2c 00 00 c5 00 79	.....|..*..}..*..~..+.. ...+.....+....$+....*+....9+.. ..J+....S+....h+....u+....{+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,....&,....9,....C,....K,.. ..Q,....V,....],....`,....a,.. ..i,....t,....y	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\sr.pak	unknown	128600	05 00 00 00 01 00 00 00 b1 06 b6 00 7c 00 10 2b 00 00 7d 00 1f 2b 00 00 7e 00 2a 2b 00 00 80 00 32 2b 00 00 81 00 37 2b 00 00 82 00 44 2b 00 00 83 00 4a 2b 00 00 84 00 59 2b 00 00 85 00 6a 2b 00 00 86 00 73 2b 00 00 88 00 88 2b 00 00 89 00 95 2b 00 00 8b 00 9b 2b 00 00 8c 00 aa 2b 00 00 8e 00 b0 2b 00 00 8f 00 c2 2b 00 00 91 00 ca 2b 00 00 92 00 cf 2b 00 00 94 00 d7 2b 00 00 9d 00 df 2b 00 00 9e 00 e7 2b 00 00 9f 00 ee 2b 00 00 a0 00 f5 2b 00 00 a3 00 fc 2b 00 00 a4 00 fd 2b 00 00 a6 00 fe 2b 00 00 a7 00 28 2c 00 00 a8 00 4b 2c 00 00 b1 00 70 2c 00 00 b4 00 98 2c 00 00 b5 00 cd 2c 00 00 b6 00 d7 2c 00 00 b7 00 e3 2c 00 00 b8 00 fc 2c 00 00 bc 00 0a 2d 00 00 bd 00 11 2d 00 00 be 00 14 2d 00 00 bf 00 15 2d 00 00 c0 00 24 2d 00 00 c2 00 3a 2d 00 00 c5 00 44	.....|..+..}..+..~.*+.. ..2+....7+....D+....J+....Y+.. ..j+....s+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+....(,....K,.. ..p,.....,.....,.....,.....,.....-.....-.....-.....-....$-....:-....D	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\sv.pak	unknown	78213	05 00 00 00 01 00 00 00 a9 06 be 00 7c 00 00 2b 00 00 7d 00 0f 2b 00 00 7e 00 1a 2b 00 00 80 00 22 2b 00 00 81 00 27 2b 00 00 82 00 34 2b 00 00 83 00 3a 2b 00 00 84 00 49 2b 00 00 85 00 5a 2b 00 00 86 00 63 2b 00 00 88 00 78 2b 00 00 89 00 85 2b 00 00 8b 00 8b 2b 00 00 8c 00 9a 2b 00 00 8e 00 a0 2b 00 00 8f 00 b2 2b 00 00 91 00 ba 2b 00 00 92 00 bf 2b 00 00 94 00 c7 2b 00 00 9d 00 cf 2b 00 00 9e 00 d7 2b 00 00 9f 00 de 2b 00 00 a0 00 e5 2b 00 00 a3 00 ec 2b 00 00 a4 00 ed 2b 00 00 a6 00 ee 2b 00 00 a7 00 ff 2b 00 00 a8 00 11 2c 00 00 b1 00 25 2c 00 00 b4 00 35 2c 00 00 b5 00 49 2c 00 00 b6 00 51 2c 00 00 b7 00 59 2c 00 00 b8 00 64 2c 00 00 bc 00 6a 2c 00 00 bd 00 71 2c 00 00 be 00 74 2c 00 00 bf 00 75 2c 00 00 c0 00 7d 2c 00 00 c2 00 88 2c 00 00 c5 00 8e	.....|..+..}..+..~..+.. ..'+....'+....4+....:+....I+.. ..Z+....c+....x+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ..%,....5,....I,....Q,....Y,.. ..d,....j,....q,....t,....u,.. ..},.....,.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\sw.pak	unknown	80058	05 00 00 00 01 00 00 00 9f 06 c8 00 7c 00 ec 2a 00 00 7d 00 fb 2a 00 00 7e 00 06 2b 00 00 80 00 0e 2b 00 00 81 00 13 2b 00 00 82 00 20 2b 00 00 83 00 26 2b 00 00 84 00 35 2b 00 00 85 00 46 2b 00 00 86 00 4f 2b 00 00 88 00 64 2b 00 00 89 00 71 2b 00 00 8b 00 77 2b 00 00 8c 00 86 2b 00 00 8e 00 8c 2b 00 00 8f 00 9e 2b 00 00 91 00 a6 2b 00 00 92 00 ab 2b 00 00 94 00 b3 2b 00 00 9d 00 bb 2b 00 00 9e 00 c3 2b 00 00 9f 00 ca 2b 00 00 a0 00 d1 2b 00 00 a3 00 d8 2b 00 00 a4 00 d9 2b 00 00 a6 00 da 2b 00 00 a7 00 ec 2b 00 00 a8 00 fc 2b 00 00 b1 00 10 2c 00 00 b4 00 2b 2c 00 00 b5 00 42 2c 00 00 b6 00 49 2c 00 00 b7 00 4e 2c 00 00 b8 00 55 2c 00 00 bc 00 5a 2c 00 00 bd 00 61 2c 00 00 be 00 64 2c 00 00 bf 00 65 2c 00 00 c0 00 6c 2c 00 00 c2 00 78 2c 00 00 c5 00 82	.....|..*..}..*..~..+.. ...+.....+.... +....&+....5+.. ..F+....O+....d+....q+....w+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,....+,....B,....I,....N,.. ..U,....Z,....a,....d,....e,.. ..l,....x,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\ta.pak	unknown	195736	05 00 00 00 01 00 00 00 a1 06 c6 00 7c 00 f0 2a 00 00 7d 00 ff 2a 00 00 7e 00 0a 2b 00 00 80 00 12 2b 00 00 81 00 17 2b 00 00 82 00 24 2b 00 00 83 00 2a 2b 00 00 84 00 39 2b 00 00 85 00 4a 2b 00 00 86 00 53 2b 00 00 88 00 68 2b 00 00 89 00 75 2b 00 00 8b 00 7b 2b 00 00 8c 00 8a 2b 00 00 8e 00 90 2b 00 00 8f 00 a2 2b 00 00 91 00 aa 2b 00 00 92 00 af 2b 00 00 94 00 b7 2b 00 00 9d 00 bf 2b 00 00 9e 00 c7 2b 00 00 9f 00 ce 2b 00 00 a0 00 d5 2b 00 00 a3 00 dc 2b 00 00 a4 00 dd 2b 00 00 a6 00 de 2b 00 00 a7 00 0c 2c 00 00 a8 00 3a 2c 00 00 b1 00 7a 2c 00 00 b4 00 b4 2c 00 00 b5 00 15 2d 00 00 b6 00 33 2d 00 00 b7 00 51 2d 00 00 b8 00 66 2d 00 00 bc 00 72 2d 00 00 bd 00 79 2d 00 00 be 00 7c 2d 00 00 bf 00 7d 2d 00 00 c0 00 90 2d 00 00 c2 00 d1 2d 00 00 c5 00 f9	.....|..*..}..*..~..+.. ...+.....+....$+....*+....9+.. ..J+....S+....h+....u+....{+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,....:,.. ..z,.....,.....-....3-....Q-....f- ....r-....y-....|-....}-.....-.....-.....	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\te.pak	unknown	184081	05 00 00 00 01 00 00 00 b3 06 b4 00 7c 00 14 2b 00 00 7d 00 23 2b 00 00 7e 00 2e 2b 00 00 80 00 36 2b 00 00 81 00 3b 2b 00 00 82 00 48 2b 00 00 83 00 4e 2b 00 00 84 00 5d 2b 00 00 85 00 6e 2b 00 00 86 00 77 2b 00 00 88 00 8c 2b 00 00 89 00 99 2b 00 00 8b 00 9f 2b 00 00 8c 00 ae 2b 00 00 8e 00 b4 2b 00 00 8f 00 c6 2b 00 00 91 00 ce 2b 00 00 92 00 d3 2b 00 00 94 00 db 2b 00 00 9d 00 e3 2b 00 00 9e 00 eb 2b 00 00 9f 00 f2 2b 00 00 a0 00 f9 2b 00 00 a3 00 00 2c 00 00 a4 00 01 2c 00 00 a6 00 02 2c 00 00 a7 00 39 2c 00 00 a8 00 6d 2c 00 00 b1 00 aa 2c 00 00 b4 00 d2 2c 00 00 b5 00 24 2d 00 00 b6 00 4b 2d 00 00 b7 00 72 2d 00 00 b8 00 99 2d 00 00 bc 00 b1 2d 00 00 bd 00 b8 2d 00 00 be 00 bb 2d 00 00 bf 00 bd 2d 00 00 c0 00 ca 2d 00 00 c2 00 f6 2d 00 00 c5 00 0b	.....|..+..}.#+..~..+.. ..6+....;+....H+....N+....]+.. ..n+....w+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....,.....,....9,....m,.. ...,.....,....$-....K-....r-.....-.....-.....-.....-.....-.....-.....-.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\th.pak	unknown	159993	05 00 00 00 01 00 00 00 8b 06 dc 00 7c 00 c4 2a 00 00 7d 00 d3 2a 00 00 7e 00 d9 2a 00 00 81 00 e1 2a 00 00 82 00 ee 2a 00 00 83 00 f4 2a 00 00 84 00 03 2b 00 00 85 00 14 2b 00 00 86 00 1d 2b 00 00 88 00 32 2b 00 00 89 00 3f 2b 00 00 8b 00 45 2b 00 00 8c 00 54 2b 00 00 8e 00 5a 2b 00 00 8f 00 6c 2b 00 00 91 00 74 2b 00 00 92 00 79 2b 00 00 93 00 81 2b 00 00 94 00 8c 2b 00 00 98 00 94 2b 00 00 9d 00 99 2b 00 00 9e 00 a1 2b 00 00 9f 00 a8 2b 00 00 a0 00 af 2b 00 00 a3 00 b6 2b 00 00 a6 00 b8 2b 00 00 a7 00 dc 2b 00 00 a8 00 06 2c 00 00 b1 00 5a 2c 00 00 b4 00 7e 2c 00 00 b5 00 c3 2c 00 00 b7 00 cc 2c 00 00 b8 00 de 2c 00 00 bc 00 e7 2c 00 00 bd 00 ee 2c 00 00 bf 00 f1 2c 00 00 c0 00 04 2d 00 00 c2 00 29 2d 00 00 c5 00 35 2d 00 00 ce 00 47 2d 00 00 dc 00 7a	.....|..*..}..*..~..*.. ...*.....*.....*.....+.....+.. ...+....2+....?+....E+....T+.. ..Z+....I+....t+....y+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ..Z,....~,.....,.....,.....,.. ...,.....,.....,.....-....)-....5- ....G-....z	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\tr.pak	unknown	82934	05 00 00 00 01 00 00 00 aa 06 bd 00 7c 00 02 2b 00 00 7d 00 11 2b 00 00 7e 00 1c 2b 00 00 80 00 24 2b 00 00 81 00 29 2b 00 00 82 00 36 2b 00 00 83 00 3c 2b 00 00 84 00 4b 2b 00 00 85 00 5c 2b 00 00 86 00 65 2b 00 00 88 00 7a 2b 00 00 89 00 87 2b 00 00 8b 00 8d 2b 00 00 8c 00 9c 2b 00 00 8e 00 a2 2b 00 00 8f 00 b4 2b 00 00 91 00 bc 2b 00 00 92 00 c1 2b 00 00 94 00 c9 2b 00 00 9d 00 d1 2b 00 00 9e 00 d9 2b 00 00 9f 00 e0 2b 00 00 a0 00 e7 2b 00 00 a3 00 ee 2b 00 00 a4 00 ef 2b 00 00 a6 00 f0 2b 00 00 a7 00 08 2c 00 00 a8 00 1e 2c 00 00 b1 00 33 2c 00 00 b4 00 49 2c 00 00 b5 00 63 2c 00 00 b6 00 7b 2c 00 00 b7 00 82 2c 00 00 b8 00 8d 2c 00 00 bc 00 92 2c 00 00 bd 00 99 2c 00 00 be 00 9c 2c 00 00 bf 00 9d 2c 00 00 c0 00 a5 2c 00 00 c2 00 b4 2c 00 00 c5 00 b8	.....|..+..}..+..~..+.. ..$+....)+....6+....<+....K+.. ..\+....e+....z+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,.....,.. ..3,....I,....c,....{,.....,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\uk.pak	unknown	137010	05 00 00 00 01 00 00 00 aa 06 bd 00 7c 00 02 2b 00 00 7d 00 11 2b 00 00 7e 00 1c 2b 00 00 80 00 24 2b 00 00 81 00 29 2b 00 00 82 00 36 2b 00 00 83 00 3c 2b 00 00 84 00 4b 2b 00 00 85 00 5c 2b 00 00 86 00 65 2b 00 00 88 00 7a 2b 00 00 89 00 87 2b 00 00 8b 00 8d 2b 00 00 8c 00 9c 2b 00 00 8e 00 a2 2b 00 00 8f 00 b4 2b 00 00 91 00 bc 2b 00 00 92 00 c1 2b 00 00 94 00 c9 2b 00 00 9d 00 d1 2b 00 00 9e 00 d9 2b 00 00 9f 00 e0 2b 00 00 a0 00 e7 2b 00 00 a3 00 ee 2b 00 00 a4 00 ef 2b 00 00 a6 00 f0 2b 00 00 a7 00 0d 2c 00 00 a8 00 26 2c 00 00 b1 00 50 2c 00 00 b4 00 7b 2c 00 00 b5 00 bd 2c 00 00 b6 00 cd 2c 00 00 b7 00 df 2c 00 00 b8 00 f1 2c 00 00 bc 00 ff 2c 00 00 bd 00 06 2d 00 00 be 00 09 2d 00 00 bf 00 0a 2d 00 00 c0 00 1d 2d 00 00 c2 00 33 2d 00 00 c5 00 3d	.....|..+..}..+..~..+.. ..$+....)+....6+....<+....K+.. ..\+....e+....z+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....,....&,.. ..P,....{,.....,.....,.....,.. ...,.....,.....-.....-.....-.....-....3- ....=	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\vi.pak	unknown	96974	05 00 00 00 01 00 00 00 9b 06 cc 00 7c 00 e4 2a 00 00 7d 00 f3 2a 00 00 7e 00 fe 2a 00 00 80 00 06 2b 00 00 81 00 0b 2b 00 00 82 00 18 2b 00 00 83 00 1e 2b 00 00 84 00 2d 2b 00 00 85 00 3e 2b 00 00 86 00 47 2b 00 00 88 00 5c 2b 00 00 89 00 69 2b 00 00 8b 00 6f 2b 00 00 8c 00 7e 2b 00 00 8e 00 84 2b 00 00 8f 00 96 2b 00 00 91 00 9e 2b 00 00 92 00 a3 2b 00 00 94 00 ab 2b 00 00 9d 00 b3 2b 00 00 9e 00 bb 2b 00 00 9f 00 c2 2b 00 00 a0 00 c9 2b 00 00 a3 00 d0 2b 00 00 a4 00 d1 2b 00 00 a6 00 d2 2b 00 00 a7 00 e3 2b 00 00 a8 00 f4 2b 00 00 b1 00 1d 2c 00 00 b4 00 46 2c 00 00 b5 00 65 2c 00 00 b6 00 6e 2c 00 00 b7 00 77 2c 00 00 b8 00 83 2c 00 00 bc 00 89 2c 00 00 bd 00 90 2c 00 00 be 00 93 2c 00 00 bf 00 94 2c 00 00 c0 00 9e 2c 00 00 c2 00 b0 2c 00 00 c5 00 ba	.....|..*..}..*..~..*.. ...+.....+.....+.....+....-+.. ..>+....G+....\+....i+....o+.. ..~+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...,.....F,....e,....n,....w,.. ...,.....,.....,.....,.....,.. ...,.....,.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\locales\zh-CN.pak	unknown	72657	05 00 00 00 01 00 00 00 83 06 e4 00 7c 00 b4 2a 00 00 7d 00 c3 2a 00 00 7e 00 ca 2a 00 00 7f 00 d2 2a 00 00 81 00 d8 2a 00 00 82 00 dd 2a 00 00 83 00 e3 2a 00 00 84 00 f2 2a 00 00 85 00 03 2b 00 00 86 00 0c 2b 00 00 88 00 21 2b 00 00 89 00 2e 2b 00 00 8e 00 34 2b 00 00 8f 00 46 2b 00 00 92 00 4e 2b 00 00 93 00 56 2b 00 00 94 00 61 2b 00 00 95 00 69 2b 00 00 98 00 78 2b 00 00 9d 00 7d 2b 00 00 9e 00 85 2b 00 00 a0 00 8c 2b 00 00 a3 00 93 2b 00 00 a6 00 95 2b 00 00 a7 00 9e 2b 00 00 a8 00 aa 2b 00 00 b1 00 bc 2b 00 00 b4 00 d1 2b 00 00 b5 00 e3 2b 00 00 b6 00 ec 2b 00 00 b7 00 f5 2b 00 00 b8 00 fb 2b 00 00 bc 00 01 2c 00 00 bd 00 08 2c 00 00 be 00 0b 2c 00 00 bf 00 0d 2c 00 00 c0 00 17 2c 00 00 c2 00 21 2c 00 00 c5 00 27 2c 00 00 ce 00 2d 2c 00 00 dc 00 39	.....|..*..}..*..~..*.. ...*.....*.....*.....*.....*.. ...+.....+....!+.....+....4+.. ..F+....N+....V+....a+....i+.. ..x+....}+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,.....,.....,.....,....!,....',....-,....9	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\locales\zh-TW.pak	unknown	72935	05 00 00 00 01 00 00 00 85 06 e2 00 7c 00 b8 2a 00 00 7d 00 c7 2a 00 00 7e 00 d2 2a 00 00 80 00 da 2a 00 00 81 00 df 2a 00 00 82 00 e7 2a 00 00 83 00 ed 2a 00 00 84 00 fc 2a 00 00 85 00 0d 2b 00 00 86 00 16 2b 00 00 88 00 2b 2b 00 00 89 00 38 2b 00 00 8b 00 3e 2b 00 00 8c 00 4d 2b 00 00 8e 00 53 2b 00 00 8f 00 65 2b 00 00 91 00 6d 2b 00 00 94 00 72 2b 00 00 9d 00 7a 2b 00 00 9e 00 82 2b 00 00 9f 00 89 2b 00 00 a0 00 90 2b 00 00 a3 00 97 2b 00 00 a6 00 99 2b 00 00 a7 00 a2 2b 00 00 a8 00 ae 2b 00 00 b1 00 bd 2b 00 00 b4 00 cf 2b 00 00 b5 00 de 2b 00 00 b6 00 ea 2b 00 00 b7 00 f6 2b 00 00 b8 00 fc 2b 00 00 bc 00 02 2c 00 00 bd 00 09 2c 00 00 be 00 0c 2c 00 00 bf 00 0e 2c 00 00 c0 00 18 2c 00 00 c2 00 28 2c 00 00 c5 00 2e 2c 00 00 ce 00 34 2c 00 00 dc 00 40	.....|..*..}..*..~..*.. ...*.....*.....*.....*.....*.. ...+.....+....++....8+....>+.. ..M+....S+....e+....m+....r+.. ..z+.....+.....+.....+.....+.. ...+.....+.....+.....+.....+.. ...+.....+.....+.....+.....,.. ...,.....,.....,.....,.....(,... ...,....4,....@	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\natives_blob.bin	unknown	82118	20 40 43 6f 6d 6d 6f 6e 4f 70 65 72 61 74 69 6f 6e 73 55 ad 0a 28 66 75 6e 63 74 69 6f 6e 28 67 6c 6f 62 61 6c 2c 20 62 69 6e 64 69 6e 67 2c 20 76 38 29 20 7b 0a 27 75 73 65 20 73 74 72 69 63 74 27 3b 0a 63 6f 6e 73 74 20 5f 71 75 65 75 65 20 3d 20 76 38 2e 63 72 65 61 74 65 50 72 69 76 61 74 65 53 79 6d 62 6f 6c 28 27 5b 5b 71 75 65 75 65 5d 5d 27 29 3b 0a 63 6f 6e 73 74 20 5f 71 75 65 75 65 54 6f 74 61 6c 53 69 7a 65 20 3d 20 76 38 2e 63 72 65 61 74 65 50 72 69 76 61 74 65 53 79 6d 62 6f 6c 28 27 5b 5b 71 75 65 75 65 54 6f 74 61 6c 53 69 7a 65 5d 5d 27 29 3b 0a 63 6f 6e 73 74 20 5f 69 73 53 65 74 74 6c 65 64 20 3d 20 76 38 2e 63 72 65 61 74 65 50 72 69 76 61 74 65 53 79 6d 62 6f 6c 28 27 69 73 53 65 74 74 6c 65 64 27 29 3b 0a 63 6f 6e 73 74 20 42 6f 6f	@CommonOperationsU.. (function(global, binding, v8) {.'use strict';.const _queue = v8.crea tePrivateSymbol('[[queue]]');.const _queueTotalSize = v8.cre atePrivateSymbol('[[queue TotalSize]]');.const _isSettled = v 8.createPrivateSymbol('isS ettled');.const Boo	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\resources.pak	unknown	1048576	05 00 00 00 01 00 00 00 d9 02 02 00 42 31 30 11 00 00 43 31 12 7b 00 00 3a 43 31 87 01 00 3b 43 3e 8b 01 00 3c 43 ba 8f 01 00 3d 43 4f 92 01 00 3e 43 9e 60 03 00 3f 43 46 64 03 00 40 43 77 69 03 00 41 43 1c 72 03 00 42 43 d1 74 03 00 43 43 99 75 03 00 44 43 a3 79 03 00 45 43 26 7c 03 00 46 43 64 89 03 00 47 43 aa 28 04 00 48 43 61 31 04 00 49 43 7f 32 04 00 4a 43 a6 33 04 00 4b 43 8f 34 04 00 4c 43 95 39 04 00 4d 43 71 3b 04 00 4e 43 91 40 04 00 4f 43 d8 45 04 00 50 43 b0 5a 04 00 51 43 06 6f 04 00 52 43 01 74 04 00 53 43 a5 75 04 00 54 43 62 7d 04 00 55 43 5d 86 04 00 56 43 b7 92 04 00 60 43 6d 6c 05 00 61 43 ff 71 05 00 62 43 89 74 05 00 63 43 2c 76 05 00 64 43 1c 7d 05 00 65 43 c6 89 05 00 66 43 09 8d 05 00 67 43 aa 8e 05 00 68 43 dd 96 05 00 69 43 d8	.....B10...C1.{..:C1... ;C>...<C....=CO...>C.`..? CFd.. @Cwi..AC.r..BC.t..CC.u..D C.y..EC&|..FCd...GC. (..HCa1..IC.2.. JC.3..KC.4..LC.9..MCq;..N C.@.. OC.E..PC.Z..QC.o..RC.t..S C.u.. TCb}..UC]...VC....`Cml..aC .q.. bC.t..cC,v..dC.}..eC....fC.... gC....hC....iC.	success or wait	9	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\resources\app-update.yml	unknown	119	6f 77 6e 65 72 3a 20 74 68 65 2d 76 69 61 0a 72 65 70 6f 3a 20 72 65 6c 65 61 73 65 73 0a 70 72 6f 76 69 64 65 72 3a 20 67 69 74 68 75 62 0a 70 75 62 6c 69 73 68 41 75 74 6f 55 70 64 61 74 65 3a 20 74 72 75 65 0a 70 72 69 76 61 74 65 3a 20 66 61 6c 73 65 0a 75 70 64 61 74 65 72 43 61 63 68 65 44 69 72 4e 61 6d 65 3a 20 76 69 61 2d 75 70 64 61 74 65 72 0a	owner: the-via.repo: releases.provider: github.publishAutoUpdate: true.private: false.updaterCacheDirName: via-updater.	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	unknown	1048576	04 00 00 00 1c 07 0c 00 18 07 0c 00 11 07 0c 00 7b 22 66 69 6c 65 73 22 3a 7b 22 70 61 63 6b 61 67 65 2e 6a 73 6f 6e 22 3a 7b 22 73 69 7a 65 22 3a 33 35 36 30 2c 22 6f 66 66 73 65 74 22 3a 22 30 22 7d 2c 22 61 70 70 22 3a 7b 22 66 69 6c 65 73 22 3a 7b 22 61 70 70 2e 68 74 6d 6c 22 3a 7b 22 73 69 7a 65 22 3a 31 32 34 38 2c 22 6f 66 66 73 65 74 22 3a 22 33 35 36 30 22 7d 2c 22 6d 61 69 6e 2e 70 72 6f 64 2e 6a 73 22 3a 7b 22 73 69 7a 65 22 3a 32 33 37 37 36 33 2c 22 6f 66 66 73 65 74 22 3a 22 34 38 30 38 22 7d 2c 22 6d 61 69 6e 2e 70 72 6f 64 2e 6a 73 2e 6d 61 70 22 3a 7b 22 73 69 7a 65 22 3a 32 38 30 36 33 37 2c 22 6f 66 66 73 65 74 22 3a 22 32 34 32 35 37 31 22 7d 2c 22 64 69 73 74 22 3a 7b 22 66 69 6c 65 73 22 3a 7b 22 30 38 34 66 37 35 38 39 66 34 62 66	.....{"files":{"package.json":{"size":3560,"offset":"0"},"app":{"files":{"app.html":{"size":1248,"offset":"3560"},"main.prod.js":{"size":237763,"offset":"4808"},"main.prod.js.map":{"size":280637,"offset":"242571"},"dist":{"files":{"084f7589f4bf	success or wait	150	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\snapshot_blob.bin	unknown	280424	01 00 00 00 01 00 00 00 1f 8b 32 15 a4 f6 db 63 37 2e 38 2e 32 37 39 2e 32 33 2d 65 6c 65 63 74 72 6f 6e 2e 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 f0 02 00 28 53 03 00 b4 03 de c0 06 00 00 00 b0 ef 02 00 00 00 00 80 00 00 00 80 e8 3e 02 80 c0 51 02 80 a0 00 00 80 00 00 00 80 00 00 00 00 60 00 00 00 00 0a 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 b9 00 00 00 60 00 00 00 00 35 00 00 00 60 00 00 00 00 fd 00 00 00 60 00 00 00 00 a9 02 00 00 1a 02 20 11 a5 07 11 6d 07 60 00 00 00 00 24 01 00 00 44 02 08 58 21 71 0e 02 08 58 21 35 0e 02 08 58 21 35 0e 44 02 20 90 11 4d 05 60 00 00 00 00 24 01 00 00 44 02 08 58 21 61 0e 02 08 58 21	.........2....c7.8.279.23-ele ctron.0...................... ....0...(S.... ....>...Q...... ....`........`........`... .....`........`....5...`...... ..`.......... ....m.`....$...D ..X!q...X!5...X!5.D. ..M.`.... $...D..X!a...X!	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\v8_context_snapshot.bin	unknown	701096	03 00 00 00 01 00 00 00 5c e0 9f 88 ac 99 83 03 37 2e 38 2e 32 37 39 2e 32 33 2d 65 6c 65 63 74 72 6f 6e 2e 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 1a 06 00 48 7d 06 00 90 71 07 00 a8 22 09 00 b4 03 de c0 08 00 00 00 c0 19 06 00 00 00 00 80 00 00 00 80 d8 fe 03 00 a8 fe 03 00 68 23 01 80 c0 51 02 80 a0 00 00 80 00 00 00 80 00 00 00 00 60 00 00 00 00 0a 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 3c 05 00 00 60 00 00 00 00 b9 00 00 00 60 00 00 00 00 35 00 00 00 60 00 00 00 00 fd 00 00 00 60 00 00 00 00 a9 02 00 00 1a 02 20 11 a5 07 11 6d 07 60 00 00 00 00 24 01 00 00 44 02 08 58 21 71 0e 02 08 58 21 35 0e 02 08 58 21 35 0e 44 02 20 90 11 4d 05 60 00 00 00	........\.......7.8.279.23-ele ctron.0...................... ....P...H}...q ..."......................... ....h#...Q.............`..... ...`........`....<...`........ `....5...`........`.......... ....m.`....$...D..X!q...X!5... X!5.D. ..M.`...	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	unknown	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 eb 08 cd 0f af 69 a3 5c af 69 a3 5c af 69 a3 5c 4b 32 a6 5d 96 69 a3 5c 4b 32 a7 5d ae 69 a3 5c f4 01 a2 5d ad 69 a3 5c a6 11 30 5c a0 69 a3 5c af 69 a2 5c 20 6d a3 5c f4 01 a0 5d ab 69 a3 5c f4 01 a6 5d b2 69 a3 5c f4 01 a7 5d a3 69 a3 5c f4 01 a3 5d ae 69 a3 5c f4 01 aa 5d 27 69 a3 5c f4 01 5e 5c ad 69 a3 5c f4 01 5c 5c ae 69 a3 5c f4 01 a1 5d ae 69 a3 5c 52 69 63 68 af 69 a3	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $...........i.\.i.\.i.\K2.].i .\K2.].i.\...].i.\..0\.i.\.i.\ m.\...].i.\...].i.\...].i.\.. .].i.\...]'i.\..^\.i.\..\\.i.\ ...].i.\Rich.i.	success or wait	17	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\d3dcompiler_47.dll	unknown	25544	10 a1 18 a1 20 a1 28 a1 30 a1 38 a1 40 a1 48 a1 50 a1 58 a1 60 a1 e0 a2 40 a3 a0 a3 00 a4 60 a4 c0 a4 20 a5 80 a5 e0 a5 40 a6 a0 a6 00 a7 60 a7 c0 a7 20 a8 80 a8 e0 a8 40 a9 a0 a9 00 aa 60 aa 20 ae 80 ae e0 ae 40 af a0 af 00 00 00 e0 34 00 44 00 00 00 00 a0 e0 a1 40 a2 a0 a2 00 a3 c0 a3 20 a4 80 a4 40 a5 a0 a5 00 a6 60 a6 c0 a6 80 a7 e0 a7 40 a8 a0 a8 00 a9 c0 a9 80 aa e0 aa a0 ab 00 ac 60 ac c0 ac 20 ad 80 ad a0 ae 00 af 60 af 00 f0 34 00 f4 03 00 00 30 a0 38 a0 48 a0 50 a0 60 a0 68 a0 78 a0 80 a0 90 a0 98 a0 a8 a0 b0 a0 b8 a0 c0 a0 c8 a0 d0 a0 d8 a0 e0 a0 e8 a0 f0 a0 f8 a0 00 a1 08 a1 10 a1 18 a1 20 a1 28 a1 30 a1 38 a1 40 a1 48 a1 50 a1 58 a1 60 a1 68 a1 70 a1 78 a1 80 a1 88 a1 90 a1 98 a1 a0 a1 a8 a1 b0 a1 b8 a1 c0 a1 c8 a1 d0 a1 d8 a1 e0 a1 e8 a1 f0	.... .(.0.8.@.H.P.X.`...@..... `... .....@.....`... .....@.....`. .....@.......4.D.......@....... ...@.....`.......@..............`... ....`...4... ..0.8.H.P.`.h.x.............. ....(.0.8. @.H.P.X.`.h.p.x..............	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\ffmpeg.dll	unknown	262144	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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 86 06 00 2c 93 fb 5d 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 00 00 4e 19 00 00 2a 07 00 00 00 00 00 00 0a 17 00 00 10 00 00 00 00 00 80 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 20 33 00 00 04 00 00 00 00 00 00 03 00 60 01 00 00 10 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.$..PE..d...,..]..........." .....N...*......................... .... 3....... ....`........................	success or wait	8	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\ffmpeg.dll	unknown	31744	dc 6a 1f 00 1e c8 0e 00 d5 c9 0e 00 d4 74 1f 00 d5 c9 0e 00 8c cb 0e 00 d4 74 1f 00 8c cb 0e 00 9b cc 0e 00 58 76 1f 00 9b cc 0e 00 a4 cd 0e 00 58 76 1f 00 a4 cd 0e 00 b1 ce 0e 00 58 76 1f 00 b1 ce 0e 00 8d cf 0e 00 40 68 1f 00 8d cf 0e 00 26 d0 0e 00 ec 74 1f 00 26 d0 0e 00 a9 d0 0e 00 54 68 1f 00 a9 d0 0e 00 2c d1 0e 00 54 68 1f 00 2c d1 0e 00 af d1 0e 00 54 68 1f 00 b0 d1 0e 00 13 d3 0e 00 40 68 1f 00 13 d3 0e 00 c8 d6 0e 00 dc 6a 1f 00 c8 d6 0e 00 6d d7 0e 00 00 7d 1f 00 6d d7 0e 00 61 d8 0e 00 10 7d 1f 00 61 d8 0e 00 a7 d9 0e 00 28 7d 1f 00 a7 d9 0e 00 da da 0e 00 28 7d 1f 00 da da 0e 00 5c dc 0e 00 28 7d 1f 00 5c dc 0e 00 c4 dd 0e 00 50 7d 1f 00 c4 dd 0e 00 12 e0 0e 00 78 7d 1f 00 12 e0 0e 00 18 e1 0e 00 e8 70 1f 00 18 e1 0e 00 f3 e1 0e 00 a0 7d 1f	.j...........t...........t.... ......Xv..........Xv.......... Xv..........@h......&....t..&. ......Th......,...Th..,....... Th..........@h...........j.... ..m....}..m...a....}..a....... (}..........(}......\...(}..\. ......P}..........x}.......... .p...........}.	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\libEGL.dll	unknown	141824	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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 86 08 00 2c 93 fb 5d 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 00 00 3e 01 00 00 e8 00 00 00 00 00 00 b0 38 00 00 00 10 00 00 00 00 00 80 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 a0 02 00 00 04 00 00 00 00 00 00 03 00 60 01 00 00 10 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.$..PE..d...,..].........." .....>...........8................. ....`.........................	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\libGLESv2.dll	unknown	262144	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 86 08 00 2c 93 fb 5d 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 00 00 78 4c 00 00 7c 29 00 00 00 00 00 b8 7d 49 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 90 df 00 00 04 00 00 00 00 00 00 03 00 60 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx....................@..... .... x...........!..L.!This program cannot be run in DOS mode.$..PE..d...,..].........." .....xL..|)......}I................ ....`.........................	success or wait	29	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\libGLESv2.dll	unknown	129024	18 60 39 00 a6 62 39 00 40 03 6d 00 b4 62 39 00 fc 62 39 00 18 cc 6c 00 04 63 39 00 37 64 39 00 54 03 6d 00 38 64 39 00 63 65 39 00 d0 00 6d 00 64 65 39 00 8a 8c 39 00 64 03 6d 00 8a 8c 39 00 0f 8d 39 00 14 ce 6c 00 0f 8d 39 00 05 8e 39 00 c0 02 6d 00 05 8e 39 00 24 8f 39 00 c8 d1 6c 00 24 8f 39 00 b2 90 39 00 ac ca 6c 00 b2 90 39 00 e3 92 39 00 44 df 6c 00 e3 92 39 00 d8 94 39 00 ac ca 6c 00 d8 94 39 00 06 9f 39 00 a8 01 6d 00 06 9f 39 00 e4 9f 39 00 a8 cb 6c 00 e4 9f 39 00 4c a0 39 00 c8 cc 6c 00 4c a0 39 00 67 a1 39 00 ac cf 6c 00 67 a1 39 00 c9 a1 39 00 f8 d0 6c 00 ca a1 39 00 b9 a3 39 00 88 cc 6c 00 ba a3 39 00 19 a4 39 00 58 ce 6c 00 19 a4 39 00 c1 a5 39 00 80 03 6d 00 c4 a5 39 00 34 a7 39 00 7c ca 6c 00 34 a7 39 00 64 a9 39 00 90 cd 6c 00 64 a9 39	.`9..b9.@.m..b9..b9...l..c9.7d 9.T.m.8d9.ce9...m.de9...9.d.m. ..9...9...l...9...9...m...9.$. 9...l.$.9...9...l...9...9.D.l. ..9...9...l...9...9...m...9... 9...l...9.L.9...l.L.9.g.9...l. g.9...9...l...9...9...l...9... 9.X.l...9...9...m...9.4.9.|.l. 4.9.d.9...l.d.9	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\resources\elevate.exe	unknown	107520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 42 e4 f7 4f 06 85 99 1c 06 85 99 1c 06 85 99 1c b2 19 68 1c 0f 85 99 1c b2 19 6a 1c 71 85 99 1c b2 19 6b 1c 1e 85 99 1c 65 d8 9a 1d 17 85 99 1c 65 d8 9c 1d 18 85 99 1c 65 d8 9d 1d 17 85 99 1c db 7a 52 1c 01 85 99 1c 06 85 98 1c 5f 85 99 1c 68 d8 91 1d 07 85 99 1c 68 d8 66 1c 07 85 99 1c 06 85 0e 1c 07 85 99 1c 68 d8 9b 1d 07 85 99 1c 52 69 63 68 06 85 99 1c 00 00 00 00 00 00 00 00	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.....	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\swiftshader\libEGL.dll	unknown	262144	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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 86 08 00 2c 93 fb 5d 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 00 00 64 03 00 00 ce 01 00 00 00 00 00 44 98 02 00 00 10 00 00 00 00 00 80 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 a0 05 00 00 04 00 00 00 00 00 00 03 00 60 01 00 00 10 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.$..PE..d...,..]..........'' .....d..........D.................. ....`.........................	success or wait	1	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\swiftshader\libEGL.dll	unknown	79360	38 23 04 80 01 00 00 00 59 00 00 00 00 00 00 00 38 03 04 80 01 00 00 00 3c 00 00 00 00 00 00 00 00 48 23 04 80 01 00 00 00 85 00 00 00 00 00 00 00 58 23 04 80 01 00 00 00 a7 00 00 00 00 00 00 00 68 23 04 80 01 00 00 00 76 00 00 00 00 00 00 00 78 23 04 80 01 00 00 00 9c 00 00 00 00 00 00 00 20 02 04 80 01 00 00 00 19 00 00 00 00 00 00 00 88 23 04 80 01 00 00 00 5b 00 00 00 00 00 00 00 68 02 04 80 01 00 00 00 22 00 00 00 00 00 00 00 98 23 04 80 01 00 00 00 64 00 00 00 00 00 00 00 a8 23 04 80 01 00 00 00 be 00 00 00 00 00 00 00 b8 23 04 80 01 00 00 00 c3 00 00 00 00 00 00 00 c8 23 04 80 01 00 00 00 b0 00 00 00 00 00 00 00 d8 23 04 80 01 00 00 00 b8 00 00 00 00 00 00 00 e8 23 04 80 01 00 00 00 cb 00 00 00 00 00 00 00 f8 23 04 80 01 00 00 00 c7 00 00 00 00 00 00	8#......Y.......8.......<..... ..H#..............X#.......... ....h#......v.......x#............. ....#...... [.......h......."........#.... ..d........#...............#.. ....#...............# ....#.............. .#.............	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\swiftshader\libGLESv2.dll	unknown	262144	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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 86 08 00 2c 93 fb 5d 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 00 00 ac 34 00 00 ee 05 00 00 00 00 00 e8 cd 31 00 00 10 00 00 00 00 00 80 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 f0 3f 00 00 04 00 00 00 00 00 00 03 00 60 01 00 00 10 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.$..PE..d...,..]..........'' ......4...........1................. ....?....... ....`.........................	success or wait	14	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\swiftshader\libGLESv2.dll	unknown	171520	e6 54 55 55 55 55 b5 3f 00 00 00 00 00 00 00 00 d4 c6 ba 99 99 99 89 3f 00 00 00 00 00 00 00 00 9f 51 f1 07 23 49 62 3f 00 00 00 00 00 00 00 00 f0 ff 5d c8 34 80 3c 3f 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 9e bd 5b 3f 00 00 00 70 d4 af 6b 3f 00 00 00 60 95 b9 74 3f 00 00 00 a0 76 94 7b 3f 00 00 00 a0 4d 34 81 3f 00 00 00 50 08 9b 84 3f 00 00 00 c0 71 fe 87 3f 00 00 00 80 90 5e 8b 3f 00 00 00 f0 6a bb 8e 3f 00 00 00 a0 83 0a 91 3f 00 00 00 e0 b5 b5 92 3f 00 00 00 50 4f 5f 94 3f 00 00 00 00 53 07 96 3f 00 00 00 d0 c3 ad 97 3f 00 00 00 f0 a4 52 99 3f 00 00 00 20 f9 f5 9a 3f 00 00 00 70 c3 97 9c 3f 00 00 00 a0 06 38 9e 3f 00 00 00 b0 c5 d6 9f	.TUUUU.?...............?...... ...Q..#Ib?..........].4.<?.... ....[?...p..k? ...`..t?....v.{?....M4.?...P.. .?....q..?.....^.?....j..?.... ...?.......?...PO_.?....S..?.. .....?.....R.?... ...?...p...? .....8.?.......	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\VIA.exe	unknown	262144	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 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 86 0d 00 2c 93 fb 5d 00 46 41 06 00 00 00 00 f0 00 22 00 0b 02 0e 00 00 76 e2 04 00 cc 5e 01 00 00 00 00 a0 05 de 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 c0 4d 06 00 04 00 00 00 00 00 00 02 00 60 c1 00 00 10 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.$.. PE..d...,..].FA......."......v ....^................@........ ....M....... ....`.........................	success or wait	400	7028124F	WriteFile
C:\Users\user\AppData\Local\Programs\via\VIA.exe	unknown	83968	f0 aa 00 ab 08 ab 10 ab 18 ab 20 ab 30 ab 38 ab 40 ab 48 ab 50 ab 60 ab 68 ab 70 ab 78 ab 80 ab 88 ab 90 ab 98 ab a0 ab a8 ab b0 ab b8 ab 00 ac 08 ac 10 ac 18 ac 20 ac 28 ac 30 ac 38 ac 40 ac 48 ac 50 ac 58 ac 50 af 58 af 60 af 68 af 70 af 78 af 80 af 00 a0 d7 05 3c 01 00 00 30 a4 38 a4 40 a4 48 a4 50 a4 58 a4 60 a4 70 a4 78 a4 80 a4 88 a4 b0 a5 b8 a5 c0 a5 c8 a5 d0 a5 d8 a5 e0 a5 e8 a5 f0 a5 f8 a5 00 a6 08 a6 10 a6 18 a6 20 a6 28 a6 30 a6 38 a6 40 a6 48 a6 50 a6 58 a6 60 a6 68 a6 70 a6 78 a6 80 a6 88 a6 90 a6 20 a7 28 a7 30 a7 38 a7 40 a7 48 a7 50 a7 a0 a9 a8 a9 b0 a9 b8 a9 c0 a9 c8 a9 d0 a9 d8 a9 e0 a9 e8 a9 f0 a9 f8 a9 00 aa 08 aa 10 aa 18 aa 20 aa 28 aa 30 aa 38 aa 40 aa 48 aa 50 aa 58 aa 60 aa 68 aa 70 aa 78 aa 80 aa 88 aa 90 aa a0 aa a8 aa b0 aa b8	.... .0.8.@.H.P.`.h.p.x. ........................ .(.0. 8.@.H.P.X.P.X.`.h.p.x....... <. ..0.8.@.H.P.X.`.p.x........... ...................... .(.0.8. @.H.P.X.`.h.p.x....... .(.0.8. @.H.P......................... ....(.0.8.@.H.P.X.`.h.p. x..............	success or wait	1	7028124F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe	unknown	23919	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c ed 6f 5a 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 68 00 00 00 38 07 00 00 40 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pf..Pf..Pf.*_9..P f..Pg.LPf.*_;..Pf..sV..Pf..V`. .Pf.Rich.Pf.................. ......PE..L...|.oZ........... .....h...8...@.	success or wait	19	405E7C	WriteFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\WinShell.dll	unknown	3072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 af fc ca c9 eb 9d a4 9a eb 9d a4 9a eb 9d a4 9a cc 5b df 9a ee 9d a4 9a eb 9d a5 9a ef 9d a4 9a cc 5b d6 9a ea 9d a4 9a cc 5b de 9a ea 9d a4 9a cc 5b dc 9a ea 9d a4 9a 52 69 63 68 eb 9d a4 9a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 c8 cd 31 54 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 08 00 00 06 00 00 00 02 00 00 00 00 00 00 ff 12 00 00 00 10 00 00 00 20 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........................ [...............[.......[.......[.. ....Rich............PE..L..... 1T.........."!.........................	success or wait	1	405E7C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\via-1.3.1-win.exe	unknown	512	success or wait	2988	405E4D	ReadFile
C:\Users\user\Desktop\via-1.3.1-win.exe	unknown	4	success or wait	3	405E4D	ReadFile
C:\Users\user\Desktop\via-1.3.1-win.exe	unknown	4	success or wait	2	405E4D	ReadFile
C:\Users\user\Desktop\via-1.3.1-win.exe	unknown	4	success or wait	4	405E4D	ReadFile
C:\Users\user\Desktop\via-1.3.1-win.exe	unknown	4	success or wait	2212	405E4D	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	1024	success or wait	1	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	32	success or wait	1	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	37	success or wait	1	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	159764	success or wait	11	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	1048576	success or wait	92	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	2866	success or wait	6	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	38130	success or wait	15	702810C7	ReadFile
C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\app-64.7z	unknown	366517	success or wait	27	702810C7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\4cee3971-2306-5318-a68a-af72635cc55f	success or wait	1	406184	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	success or wait	1	406184	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\4cee3971-2306-5318-a68a-af72635cc55f	InstallLocation	unicode	C:\Users\user\AppData\Local\Programs\via	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\4cee3971-2306-5318-a68a-af72635cc55f	KeepShortcuts	unicode	true	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\4cee3971-2306-5318-a68a-af72635cc55f	ShortcutName	unicode	VIA	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	DisplayName	unicode	VIA 1.3.1	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	UninstallString	unicode	"C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe" /currentuser	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	QuietUninstallString	unicode	"C:\Users\user\AppData\Local\Programs\via\Uninstall VIA.exe" /currentuser /S	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	DisplayVersion	unicode	1.3.1	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	DisplayIcon	unicode	C:\Users\user\AppData\Local\Programs\via\VIA.exe,0	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	Publisher	unicode	Olivia	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	NoModify	dword	1	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	NoRepair	dword	1	success or wait	1	402475	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4cee3971-2306-5318-a68a-af72635cc55f}	EstimatedSize	dword	304063	success or wait	1	402475	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	success or wait	1	406090	MoveFileExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\?? \C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll	\?? \C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\nsProcess.dll\?? \C:\Users\user\AppData\Local\Temp\nsxBEE4.tmp\	success or wait	1	406090	MoveFileExW

Analysis Process: VIA.exe PID: 6868 Parent PID: 3388

General

Start time:	05:34:37
Start date:	12/02/2021
Path:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Local\Programs\via\VIA.exe'
Imagebase:	0x7ff7e75a0000
File size:	104941568 bytes
MD5 hash:	0474F56BEB38D2AF8C20BB44D66CEBCA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\VIA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\VIA\logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7EC39C010	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7EC39C010	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\config.json.1716479925	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | open for backup ident	success or wait	1	7FF7EB7C599C	CreateFileW
C:\Users\user\AppData\Roaming\VIA\lockfile	read attributes | delete | synchronize | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FF7E76D8150	CreateFileW
C:\Users\user\AppData\Roaming\VIA\Code Cache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\Code Cache\js	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\GPUCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\GPUCache\index	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_0	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_2	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7EC39C010	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\logs\main.log	append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | open for backup ident	success or wait	1	7FF7EB7C599C	CreateFileW
C:\Users\user\AppData\Roaming\VIA\blob_storage	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\blob_storage\ec94c19a-6566-48de-89ea-73626a0b0206	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index-dir	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7E938547B	CreateDirectoryW
C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index-dir\temp-index	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW
C:\Users\user\AppData\Roaming\VIA\.updaterId	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | open for backup ident	success or wait	1	7FF7EB7C599C	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\config.json.1716479925	C:\Users\user\AppData\Roaming\VIA\config.jsonpa	success or wait	1	7FF7EB7C7A87	MoveFileExW
C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index-dir\temp-index	C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index-dir\the-real-index	success or wait	1	7FF7E93868C3	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\config.json.1716479925	0	408	7b 0a 09 22 72 65 6d 6f 74 65 44 61 74 61 22 3a 20 7b 0a 09 09 22 67 65 6e 65 72 61 74 65 64 41 74 22 3a 20 2d 31 2c 0a 09 09 22 64 65 66 69 6e 69 74 69 6f 6e 73 22 3a 20 7b 7d 2c 0a 09 09 22 74 68 65 6d 65 22 3a 20 7b 0a 09 09 09 22 61 6c 70 68 61 22 3a 20 7b 0a 09 09 09 09 22 63 22 3a 20 22 23 33 36 33 34 33 34 22 2c 0a 09 09 09 09 22 74 22 3a 20 22 23 45 38 43 34 42 38 22 0a 09 09 09 7d 2c 0a 09 09 09 22 6d 6f 64 22 3a 20 7b 0a 09 09 09 09 22 63 22 3a 20 22 23 33 36 33 34 33 34 22 2c 0a 09 09 09 09 22 74 22 3a 20 22 23 45 38 43 34 42 38 22 0a 09 09 09 7d 2c 0a 09 09 09 22 61 63 63 65 6e 74 22 3a 20 7b 0a 09 09 09 09 22 63 22 3a 20 22 23 45 38 43 34 42 38 22 2c 0a 09 09 09 09 22 74 22 3a 20 22 23 33 36 33 34 33 34 22 0a 09 09 09 7d 0a 09 09 7d 0a 09 7d	{.."remoteData": {..."generatedAt": -1,..."definitions": {}, ..."theme": {...."alpha": {... .."c": "#363434",....."t": "#E8C4B8"....},....."mod": {....."c": "#363434",....."t": "#E8C4 B8"....},....."accent": {....." c": "#E8C4B8",....."t": "#363434"....}...}..}	success or wait	1	7FF7EB7C5D55	WriteFile
C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index	0	24	30 5c 72 a7 1b 6d fb fc 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0\r..m.....	success or wait	1	7FF7E9389ED3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\GPUCache\index	0	368	c3 ca 03 c1 00 00 02 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 00 00 00 00 00 00 00 00 2e 70 12 fc b9 19 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....p..../............	success or wait	1	7FF7E9389ED3	WriteFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_0	0	8192	c3 ca 04 c1 00 00 02 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	............$.................	success or wait	1	7FF7E9389ED3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_1	0	8192	c3 ca 04 c1 00 00 02 00 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	7FF7E9389ED3	WriteFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_2	0	8192	c3 ca 04 c1 00 00 02 00 02 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	7FF7E9389ED3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_3	0	8192	c3 ca 04 c1 00 00 02 00 03 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	7FF7E9389ED3	WriteFile
C:\Users\user\AppData\Roaming\VIA\logs\main.log	unknown	54	5b 32 30 32 31 2d 30 32 2d 31 32 20 30 35 3a 33 34 3a 35 34 2e 32 30 30 5d 20 5b 69 6e 66 6f 5d 20 43 68 65 63 6b 69 6e 67 20 66 6f 72 20 75 70 64 61 74 65 0d 0a	[2021-02-12 05:34:54.200] [info] Checking for update..	success or wait	1	7FF7EB7C5D55	WriteFile
C:\Users\user\AppData\Roaming\VIA\Code Cache\js\index-dir\temp-index	0	48	28 00 00 00 50 4a 1a 5a 6f 79 20 72 65 74 6e 65 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 81 76 16 fc b9 19 2f 00	(...PJ.Zoy retne............. ....v..../.	success or wait	1	7FF7E9389ED3	WriteFile
C:\Users\user\AppData\Roaming\VIA\logs\main.log	unknown	102	5b 32 30 32 31 2d 30 32 2d 31 32 20 30 35 3a 33 34 3a 35 34 2e 33 39 38 5d 20 5b 69 6e 66 6f 5d 20 47 65 6e 65 72 61 74 65 64 20 6e 65 77 20 73 74 61 67 69 6e 67 20 75 73 65 72 20 49 44 3a 20 39 38 66 30 30 35 62 35 2d 65 38 35 39 2d 35 61 39 64 2d 39 30 61 64 2d 65 62 65 61 37 32 62 65 31 32 34 32 0d 0a	[2021-02-12 05:34:54.398] [info] Generated new staging user ID: 98f005b5-e859-5a9d-90ad-eb ea72be1242..	success or wait	1	7FF7EB7C5D55	WriteFile
C:\Users\user\AppData\Roaming\VIA\.updaterId	0	36	39 38 66 30 30 35 62 35 2d 65 38 35 39 2d 35 61 39 64 2d 39 30 61 64 2d 65 62 65 61 37 32 62 65 31 32 34 32	98f005b5-e859-5a9d-90ad-ebea72be1242	success or wait	1	7FF7EB7C5D55	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_1	8192	296	e0 27 14 f0 28 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.'..(........................	success or wait	1	7FF7E9389ED3	WriteFile
C:\Users\user\AppData\Roaming\VIA\logs\main.log	unknown	126	5b 32 30 32 31 2d 30 32 2d 31 32 20 30 35 3a 33 36 3a 31 33 2e 38 36 33 5d 20 5b 69 6e 66 6f 5d 20 55 70 64 61 74 65 20 66 6f 72 20 76 65 72 73 69 6f 6e 20 31 2e 33 2e 31 20 69 73 20 6e 6f 74 20 61 76 61 69 6c 61 62 6c 65 20 28 6c 61 74 65 73 74 20 76 65 72 73 69 6f 6e 3a 20 31 2e 33 2e 31 2c 20 64 6f 77 6e 67 72 61 64 65 20 69 73 20 64 69 73 61 6c 6c 6f 77 65 64 29 2e 0d 0a	[2021-02-12 05:36:13.863] [info] Update for version 1.3.1 is not available (latest version: 1.3.1, downgrade is disallow ed)...	success or wait	1	7FF7EB7C5D55	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	unknown	8	success or wait	2	7FF7E9385FC5	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	unknown	788252	success or wait	2	7FF7E9385FC5	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	788260	3560	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	793068	237763	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	65300575	681	success or wait	6	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	65457206	4997	success or wait	6	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	58835329	4445	success or wait	14	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Roaming\VIA\config.json	unknown	408	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Roaming\VIA\config.json	unknown	408	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	4096	success or wait	2	7FF7EC398661	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	4096	end of file	2	7FF7EC398661	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\index	0	4096	success or wait	1	7FF7E9389D69	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\index	0	262512	success or wait	1	7FF7E9389D69	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_0	0	8192	success or wait	1	7FF7E9389D69	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_0	0	8192	success or wait	1	7FF7E9389D69	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_1	0	8192	success or wait	1	7FF7E9389D69	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_2	0	8192	success or wait	1	7FF7E9389D69	ReadFile
C:\Users\user\AppData\Roaming\VIA\GPUCache\data_3	0	8192	success or wait	1	7FF7E9389D69	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	65422698	10915	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	153713161	947	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	153719939	5930	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	71461541	713	success or wait	2	7FF7EB7C5BDA	ReadFile
C:\Windows\System32\spool\drivers\color\sRGB Color Space Profile.icm	unknown	4096	success or wait	1	7FF7EC398661	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	unknown	8	success or wait	1	7FF7E9385FC5	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app-update.yml	unknown	119	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	65469347	2964	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Windows\System32\spool\drivers\color\sRGB Color Space Profile.icm	unknown	4096	end of file	1	7FF7EC398661	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	65500111	7833	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	65532726	4975	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	153664743	1977	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	153683661	5619	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	153590509	2779	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	791820	1024	success or wait	1	7FF7E9389D69	ReadFile
\mojo.6868.4464.1333781148708819525	0	4096	pending	1	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	pending	1	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	pending	14	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	success or wait	7	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	success or wait	9	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	pending	13	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.15353216135899732640	0	4096	pending	1	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	pending	1	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	success or wait	16	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	success or wait	23	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	pending	25	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	pending	46	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.15353216135899732640	0	4096	pending	3	7FF7E7E9CA1B	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	153701016	4308	success or wait	1	7FF7EB7C5BDA	ReadFile
C:\Users\user\AppData\Local\Programs\via\resources\app.asar	71461541	713	success or wait	1	7FF7EB7C5BDA	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: VIA.exe PID: 6376 Parent PID: 6868

General

Start time:	05:35:13
Start date:	12/02/2021
Path:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Local\Programs\via\VIA.exe' --type=gpu-process --field-trial-handle=1588,13949046230613957204,78855267791981413,131072 --disable-features=SpareRendererForSitePerProcess --gpu-preferences=KAAAAAAAAADgAAAwAAAAAAAAAYAAAAAAAEAAAAAAAAAAAAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --service-request-channel-token=10484998783080688572 --mojo-platform-channel-handle=1604 --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x7ff7e75a0000
File size:	104941568 bytes
MD5 hash:	0474F56BEB38D2AF8C20BB44D66CEBCA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
\Device\ConDrv\Connect	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert	invalid handle	1	2CFCB2CC434	NtCreateFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\mojo.6868.4464.1333781148708819525	unknown	256	success or wait	1	7FF7E7E9A667	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	success or wait	1	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	success or wait	21	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	pending	10	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	pending	12	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.8883044113899428450	0	4096	success or wait	5	7FF7E7E9CA1B	ReadFile

Analysis Process: VIA.exe PID: 6408 Parent PID: 6868

General

Start time:	05:35:45
Start date:	12/02/2021
Path:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Local\Programs\via\VIA.exe' --type=utility --field-trial-handle=1588,13949046230613957204,7885526779198114 13,131072 --disable-features=SpareRendererForSitePerProcess --lang=en-US --service-sandbox-type=network --service-request-channel-token=3061075516634477466 --mojo-platform-channel-handle=1928 /prefetch:8
Imagebase:	0x7ff7e75a0000
File size:	104941568 bytes
MD5 hash:	0474F56BEB38D2AF8C20BB44D66CEBCA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\64b781ed-dae5-406f-a7cd-fc221f9a4570.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7E937E975	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\64b781ed-dae5-406f-a7cd-fc221f9a4570.tmp	C:\Users\user\AppData\Roaming\VIA\Network Persistent Statemp	success or wait	1	7FF7E93868C3	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VIA\64b781ed-dae5-406f-a7cd-fc221f9a4570.tmp	0	59	7b 22 6e 65 74 22 3a 7b 22 6e 65 74 77 6f 72 6b 5f 71 75 61 6c 69 74 69 65 73 22 3a 7b 22 43 41 45 53 41 42 69 41 67 49 43 41 2b 50 2f 2f 2f 2f 38 42 22 3a 22 34 47 22 7d 7d 7d	{"net":{"network_qualities":{" CAESABiAgICA+P////8B":"4G"}}}	success or wait	1	7FF7E9389ED3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\mojo.6868.4464.15353216135899732640	unknown	256	success or wait	1	7FF7E7E9A667	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	success or wait	1	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	success or wait	25	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	pending	34	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	pending	35	7FF7E7E9CA1B	ReadFile
\mojo.6868.4464.9417888836529819093	0	4096	success or wait	16	7FF7E7E9CA1B	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	4096	success or wait	1	7FF7EC398661	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	4096	end of file	1	7FF7EC398661	ReadFile
\mojo.6868.4464.15353216135899732640	unknown	256	pending	3	7FF7E7E9A667	ReadFile

Analysis Process: VIA.exe PID: 4788 Parent PID: 6868

General

Start time:	05:36:30
Start date:	12/02/2021
Path:	C:\Users\user\AppData\Local\Programs\via\VIA.exe
Wow64 process (32bit):	
Commandline:	'C:\Users\user\AppData\Local\Programs\via\VIA.exe' --type=renderer --field-trial-handle=1588,13949046230613957204,788552677919811413,131072 --disable-features=SpareRendererForSitePerProcess --lang=en-US --app-path='C:\Users\user\AppData\Local\Programs\via\resources\app.asar' --node-integration --no-sandbox --no-zygote --background-color=#fff --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=16077176714480753997 --renderer-client-id=5 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1968 /prefetch:1
Imagebase:	
File size:	104941568 bytes
MD5 hash:	0474F56BEB38D2AF8C20BB44D66CEBCA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis