ID: 1496795
Cookbook: browseurl.jbs
Time: 17:53:24
Date: 21/08/2024
Version: 40.0.0 Tourmaline

Table of Contents

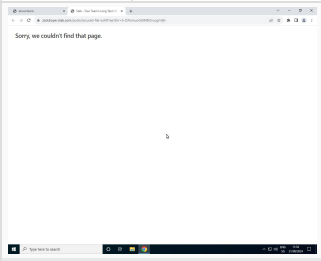
Windows Analysis Report

https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh

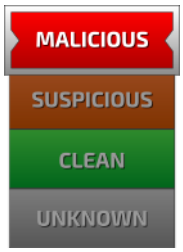
Overview

General Information

Sample URL:	http://https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh
Analysis ID:	1496795
Infos:	



Detection

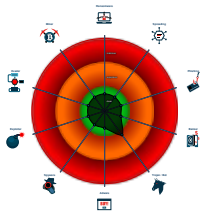


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected non-DNS traffic on DNS po…
- Stores files to the Windows start me…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1788 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 2824 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2372 --field-trial-handle=2296,i,6196848232246346782,16876402020592985407,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 4912 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

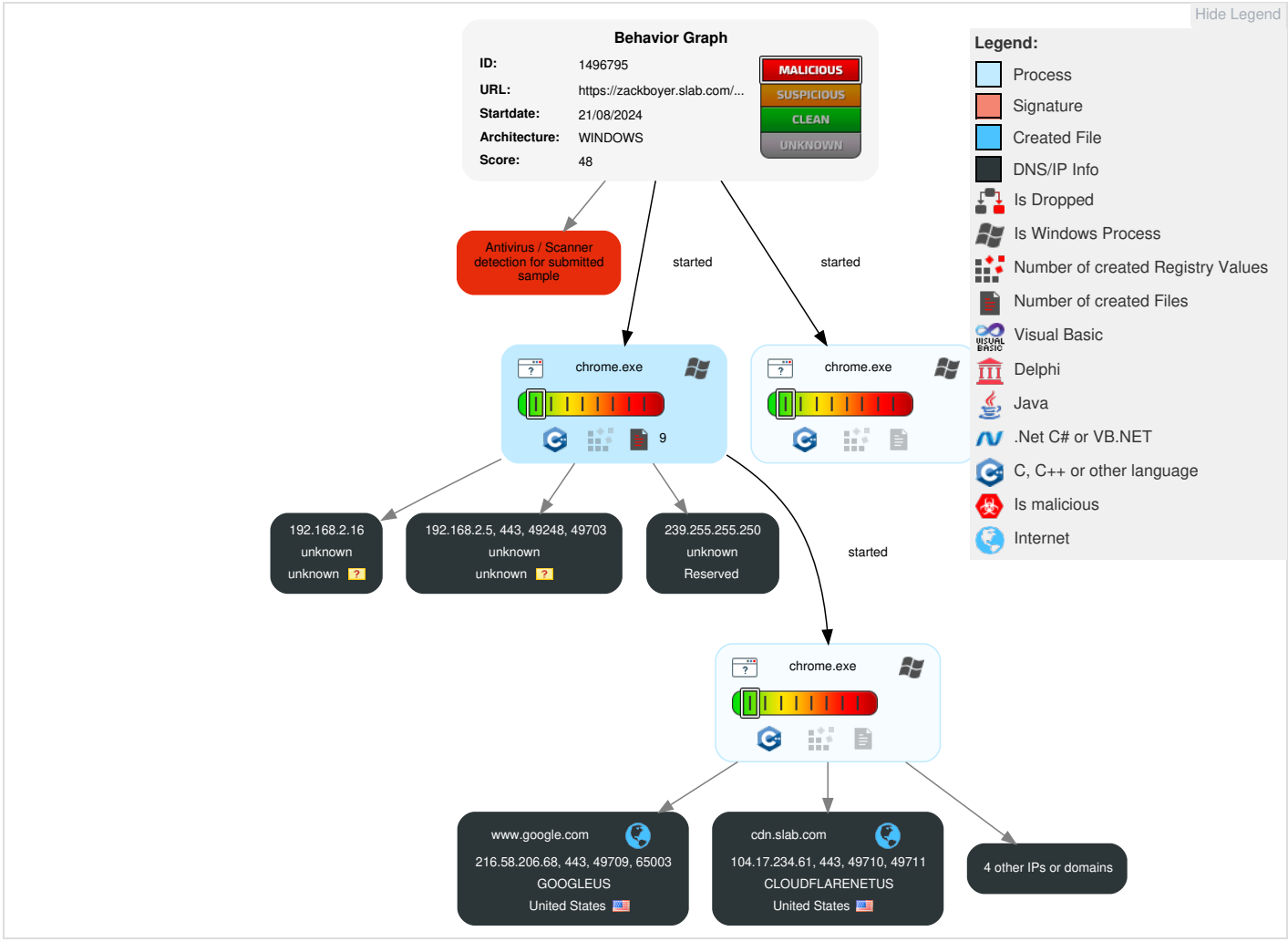
AV Detection

Antivirus / Scanner detection for submitted sample

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 Process Injection	1 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	3 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	4 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	3 Ingress Tool Transfer	Traffic Duplication	Data Destruction

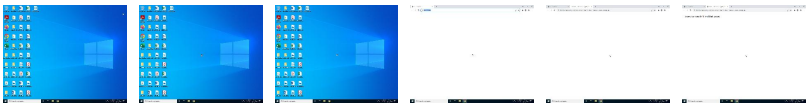
Behavior Graph

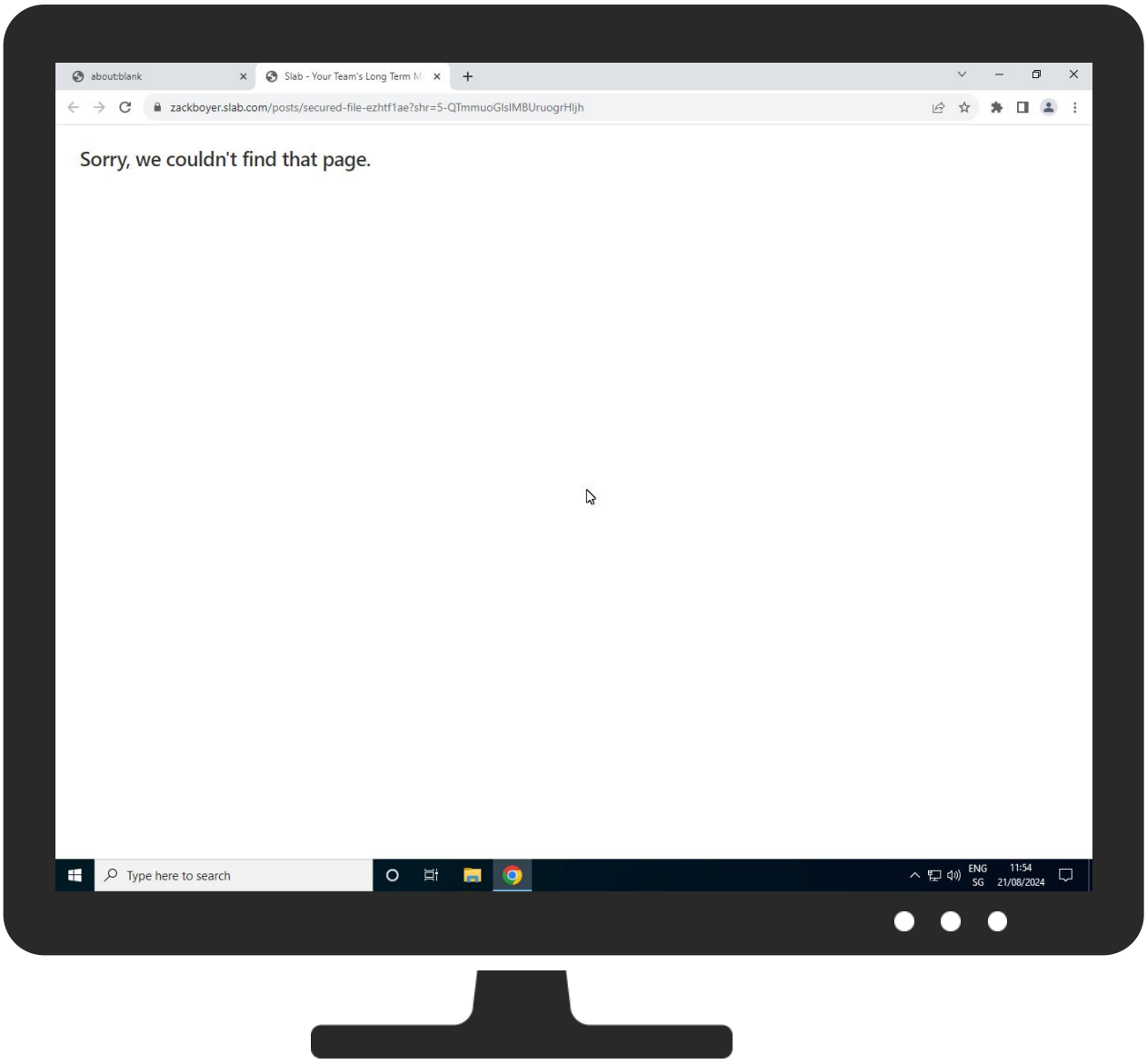


Screenshots

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
http://https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGlslMBUruogrHIjh	0%	Avira URL Cloud	safe	
http://https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGlslMBUruogrHIjh	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.segment.com/analytics.js/v1/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://bugs.webkit.org/show_bug.cgi?id=244895	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/bundles/js/workers/spellCorrector-de80abed05f7113f3fdeac0d1acc5b38.js?vsn=d	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/bundles/css/fonts/web-1982fc99f3624125665d704ac0753574.css?vsn=d	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/images/apple-touch-icon-b28ad6d7456f4246867317e5f40e6f58.png?vsn=d	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/images/favicon-4cd04a6c3329f76935c9b946f0cc2902.png?vsn=d	0%	Avira URL Cloud	safe	
http://https://github.com/gurschitz/pace/blob/528effd52440f9c20028a911b7788163abaf5f27/pace.js	0%	Avira URL Cloud	safe	
http://https://cdn.segment.com/analytics.js/v1/QfBlWGugy5p510ElBmtx2y6XsqRlyNsq/analytics.min.js	0%	Avira URL Cloud	safe	
http://https://quilljs.com	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/images/og-twitter-8201cb80a7ad72b84e436335011005d9.png?vsn=d	0%	Avira URL Cloud	safe	
http://https://github.com/CodeByZach/pace/	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/images/favicon-d8f2f390483a075c9bb320fd8c2536f8.svg?vsn=d	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/bundles/css/internal-30c3092ea9af23a639832f0b52d33537.css?vsn=d	0%	Avira URL Cloud	safe	
http://https://cdn.segment.com/v1/projects/QfBlWGugy5p510ElBmtx2y6XsqRlyNsq/settings	0%	Avira URL Cloud	safe	
http://https://cdn.slab.com/images/og-2b3858781c04dd1718e0c3abb4e13049.png?vsn=d	0%	Avira URL Cloud	safe	
http://https://github.com/KingSora	0%	Avira URL Cloud	safe	
http://https://slabstatic.com	0%	Avira URL Cloud	safe	
http://https://slab.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zackboyer.slab.com	104.17.234.61	true	false		unknown
cdn.slab.com	104.17.234.61	true	false		unknown
d296je7bbdd650.cloudfront.net	108.157.152.187	true	false		unknown
www.google.com	216.58.206.68	true	false		unknown
fp2e7a.wpc.phicdn.net	192.229.221.95	true	false		unknown
cdn.segment.com	unknown	unknown	false		unknown

Contacted URLs

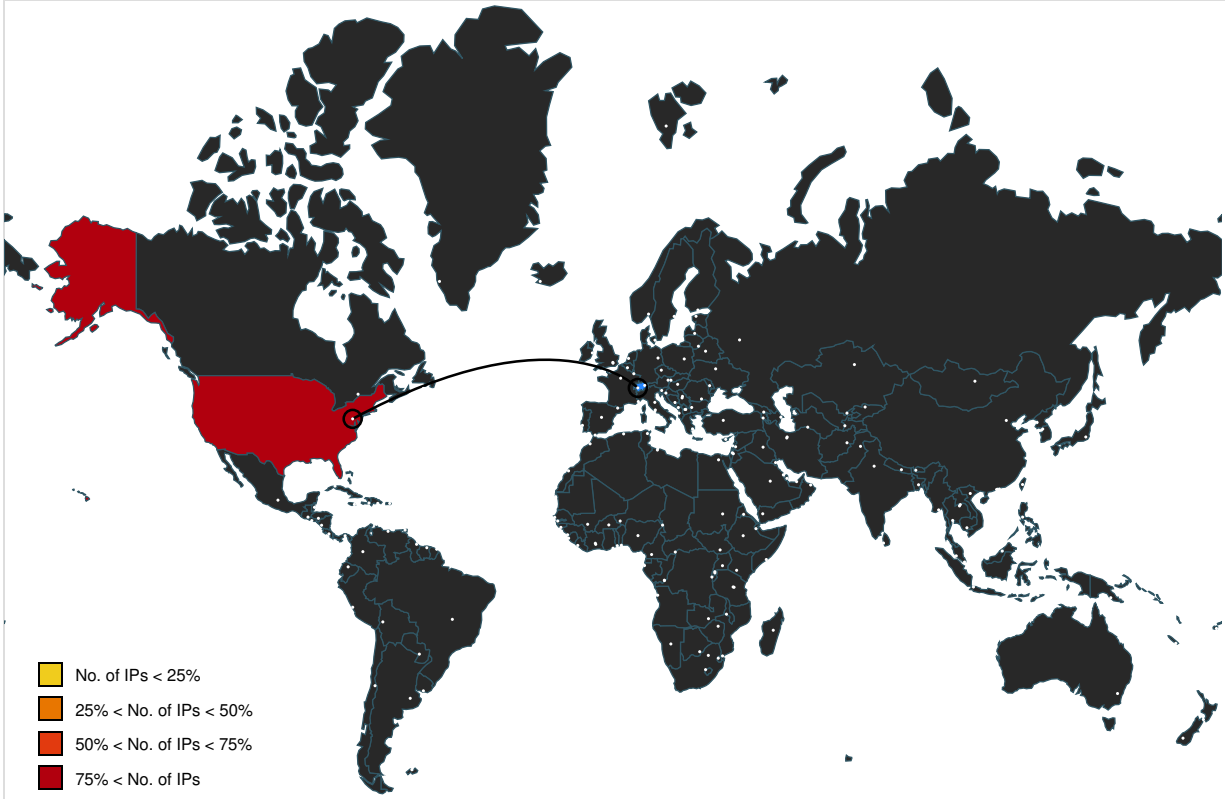
Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.slab.com/images/favicon-4cd04a6c3329f76935c9b946f0cc2902.png?vsn=d	false	• Avira URL Cloud: safe	unknown
http://https://cdn.segment.com/analytics.js/v1/QfBlWGugy5p510ElBmtx2y6XsqRlyNsq/analytics.min.js	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com/bundles/css/fonts/web-1982fc99f3624125665d704ac0753574.css?vsn=d	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com/bundles/css/internal-30c3092ea9af23a639832f0b52d33537.css?vsn=d	false	• Avira URL Cloud: safe	unknown
https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh	true		unknown
http://https://cdn.slab.com/images/favicon-d8f2f390483a075c9bb320fd8c2536f8.svg?vsn=d	false	• Avira URL Cloud: safe	unknown
http://https://cdn.segment.com/v1/projects/QfBlWGugy5p510ElBmtx2y6XsqRlyNsq/settings	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/gurschitz/pace/blob/528effd52440f9c20028a911b7788163abaf5f27/pace.js	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com/bundles/js/workers/spellCorrector-de80abed05f7113f3fdeac0d1acc5b38.js?vsn=d	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://quilljs.com	chromecache_135.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugs.webkit.org/show_bug.cgi?id=244895	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com/images/apple-touch-icon-b28ad6d7456f4246867317e5f40e6f58.png?vsn=d	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com/images/og-twitter-8201cb80a7ad72b84e436335011005d9.png?vsn=d	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/CodeByZach/pace/	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.slab.com/images/og-2b3858781c04dd1718e0c3abb4e13049.png?vsn=d	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.segment.com/analytics.js/v1/	chromecache_139.2.dr	false	• URL Reputation: safe	unknown
http://https://github.com/KingSora	chromecache_135.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://slab.com/	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://slabstatic.com	chromecache_139.2.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.157.152.187	d296je7bbdd650.cloudfront.net	United States		16509	AMAZON-02US	false
13.227.222.191	unknown	United States		16509	AMAZON-02US	false
216.58.206.68	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.234.61	zackboyer.slab.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.16
192.168.2.5

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1496795
Start date and time:	2024-08-21 17:53:24 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 3m 16s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@21/24@12/7
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.185.227, 142.250.110.84, 142.250.186.142, 34.104.35.123, 199.232.210.172, 192.229.221.95, 13.95.31.18, 52.165.164.15, 142.250.186.67
- Excluded domains from analysis (whitelisted): fs.microsoft.com, accounts.google.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.com, clients2.google.com, edgedl.me.gvt1.com, ocsp.digicert.com, ocsp.edge.digicert.com, glb.cws.prod.dcat.dsp.trafficmanager.net, update.googleapis.com, clients.l.google.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- VT rate limit hit for: https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh

Simulations

Behavior and APIs

No simulations

LLM Input / Output

Input	Output
URL: https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh Model: jbxai	{ "brand":"unknown", "has_curious_text":false, "prominent_button_name":"unknown", "text_input_field_labels":["unknown"], "pdf_icon_visible":false, "has_visible_captcha":false, "has_urgent_text":false}
Sorry, we couldn't find that page.	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Docs.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Tue Oct 3 09:48:42 2023, mtime=Wed Aug 21 14:54:27 2024, atime=Wed Sep 27 04:28:28 2023, length=1210144, window=hide
Category:	dropped
Size (bytes):	2677
Entropy (8bit):	3.981568429900043
Encrypted:	false
SSDEEP:	48:85djwTDUUHHTidAKZdA19ehwiZUklqehgy+3:8PwHX1/y
MD5:	6ED03CC2878565F8360D179BBB94C76B
SHA1:	CDBB5C37BAF1CE6DB32B8A5BB793CD4E0D038985
SHA-256:	81759463FCBCFFA0D94A9B23653800E7D4E0C94298159BF96F76637BEE193D2E
SHA-512:	1C31732DD0FCD479338BAB7004AC42505F85818CDA80B4740936F8AEEF5481101E32C74F8CD5F7B861938F299CE4AE189DBFC141A917A8B19B0E6C683DE7867
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...$+.,.....G.f....N.Yr.... w.....1....P.O. .:i.....+00.../C:\.....1.....DWWn..PROGRA~1..t.....O.I.Y.~....B.....J.....SX.P.r.o.g.r.a.m. .F.i .l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....CW.V..Google..>.....CW.V.Y.~....L.....p+j.G.o.o.g.l.e.....T.1.....CW.V..Chrome..>.....CW.V.Y.~....M..... .....8..C.h.r.o.m.e.....`.1.....CW.V..APPLIC~1..H.....CW.V.Y.~....."&.A.p.p.l.i.c.a.t.i.o.n.....n.2. w..;W.+ .CHROME~1.EXE..R.....CW.V.Y.~..... ..H..c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....C.C>.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.. ...\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o .n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Gmail.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Tue Oct 3 09:48:42 2023, mtime=Wed Aug 21 14:54:26 2024, atime=Wed Sep 27 04:28:28 2023, length=1210144, window=hide
Category:	dropped
Size (bytes):	2679
Entropy (8bit):	3.9957346717858604
Encrypted:	false
SSDEEP:	48:8HdjwTDUUHHTidAKZdA1weh/iZUkAQkqehvy+2:8RwHXv9QWy
MD5:	EF452C01C5381BBDF4794BF23E0000D1
SHA1:	58E75E99D349F06EA6CC1D1CC1B57D06F63FE091
SHA-256:	8D9B84BB23911E63090080C56030E197C15A00EDFE334057FF78CD0A9B418301
SHA-512:	5D0552EA58DCF2056FBC998D08ACD0E0B19291C8C6F24C019D0CFA473D9D872CE12D6B25161C7F64889D29DA0AABB6D20AE71F127A0C8854B68FFFA3D19C259

Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...$+.,.....z..f....N.Yr.... w.....1....P.O. .:i.....+00.../C:\.....1.....DWWn..PROGRA~1..t.....O.I.Y.~....B.....J.....SX.P.r.o.g.r.a.m. .F.i .l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....CW.V..Google..>.....CW.V.Y.~....L.....p+j.G.o.o.g.l.e.....T.1.....CW.V..Chrome..>.....CW.V.Y.~....M..... .....8..C.h.r.o.m.e.....`.1.....CW.V..APPLIC~1..H.....CW.V.Y.~....."&.A.p.p.l.i.c.a.t.i.o.n.....n.2. w..;W.+ .CHROME~1.EXE..R.....CW.V.Y.~..... ..H..c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....C.C>.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.. ...\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o .n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Google Drive.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Tue Oct 3 09:48:42 2023, mtime=Wed Oct 4 12:54:07 2023, atime=Wed Sep 27 04:28:28 2023, length=1210144, window=hide
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.006194585829049
Encrypted:	false
SSDEEP:	48:8x9djwTDUUsHTidAKZdA14tseh7sFiZUkmgqeh7sly+BX:8xzwHXmnLy
MD5:	A796015A9AE009F84453DB3550B7F8B9
SHA1:	D41457804B33D9B24B953EFC94EB9E2B12BA0D63
SHA-256:	EC44469FA77C27377C4B25CC11056592ADC0F7649EAC711B2C56E30E2276E202
SHA-512:	B5E368E7BC6FEADD9A5D5E5318CA67BF386CB85AA9D9743A0E4494592840C0E1DC4A9675A3EDB90A62B2622A77DE7B2D05262B87CDFC6258AC1524DFF4587 9B
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...$+.,.....e>....N.Yr.... w.....1....P.O. .:i.....+00.../C:\.....1.....DWWn..PROGRA~1..t.....O.I.Y.~....B.....J.....SX.P.r.o.g.r.a.m. .F.i .l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....CW.V..Google..>.....CW.V.Y.~....L.....p+j.G.o.o.g.l.e.....T.1.....CW.V..Chrome..>.....CW.V.Y.~....M..... .....8..C.h.r.o.m.e.....`.1.....CW.V..APPLIC~1..H.....CW.V.Y.~....."&.A.p.p.l.i.c.a.t.i.o.n.....n.2. w..;W.+ .CHROME~1.EXE..R.....CW.VDW.n..... ..H..c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....C.C>.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.. ...\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o .n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Sheets.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Tue Oct 3 09:48:42 2023, mtime=Wed Aug 21 14:54:26 2024, atime=Wed Sep 27 04:28:28 2023, length=1210144, window=hide
Category:	dropped
Size (bytes):	2681
Entropy (8bit):	3.994214393481015
Encrypted:	false
SSDEEP:	48:8odjwTDUUHHTidAKZdA1vehDiZUkwqehTy+R:8SwHXMNy
MD5:	F953953172F580E65635AA660D799DCB
SHA1:	02CB78B1478D84691ED73959AC7CCD593F3C6E3C
SHA-256:	B8FB598950018C60F23D5B59F8AB59C59C0B86913D9EC368393ABD40D352527D
SHA-512:	240EB3B058A5B457D7F022E5ECECB90B0239134908A73623FFB338D1757FE472098A78F750F2757BA004C47E6DF4B4DE5669EF17ADC81EE8EDAD4CD738F0602 5
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...$+.,.....n.f....N.Yr.... w.....1....P.O. .:i.....+00.../C:\.....1.....DWWn..PROGRA~1..t.....O.I.Y.~....B.....J.....SX.P.r.o.g.r.a.m. .F.i. l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....CW.V..Google..>.....CW.V.Y.~....L.....p+j.G.o.o.g.l.e.....T.1.....CW.V..Chrome..>.....CW.V.Y.~....M..... .....8..C.h.r.o.m.e.....`.1.....CW.V..APPLIC~1..H.....CW.V.Y.~....."&.A.p.p.l.i.c.a.t.i.o.n.....n.2. w..;W.+ .CHROME~1.EXE..R.....CW.V.Y.~..... .H..c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....C.C>.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.. ..\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o. n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\Slides.lnk

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Tue Oct 3 09:48:42 2023, mtime=Wed Aug 21 14:54:27 2024, atime=Wed Sep 27 04:28:28 2023, length=1210144, window=hide
Category:	dropped
Size (bytes):	2681
Entropy (8bit):	3.9818470190176325
Encrypted:	false
SSDEEP:	48:8XdjwTDUUHHTidAKZdA1hehBiZUk1W1qehBy+C:8BwHX89hy
MD5:	2FF1E90F76F3840AA9576102D278375D

SHA1:	7696B29B4F0624978D6137502979275FA47822D6
SHA-256:	60E96CDE284A6504E0CBC48C3E6EF7496C802173A2471747FA789FF09C2140B9
SHA-512:	0E29F81F8021C7A9D0EBB0B1ED3271A70B12934C981BF15404AADF9FA52DD62BD08F3B598C7DDA05C02D5FDE0FA810584BCAB7971917A65B1D06B22DBBAA935E
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...$+.,....i..f....N.Yr.... w.....1....P.O. .:i.....+00.../C:\.....1.....DWWn..PROGRA~1..t.....O.I.Y.~....B.....J.....SX.P.r.o.g.r.a.m. .F.i .l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....CW.V..Google..>.....CW.V.Y.~....L.....p+j.G.o.o.g.l.e.....T.1.....CW.V..Chrome..>.....CW.V.Y.~....M..... .....8..C.h.r.o.m.e.....`.1.....CW.V..APPLIC~1..H.....CW.V.Y.~....."&.A.p.p.l.i.c.a.t.i.o.n.....n.2. w..;W.+ .CHROME~1.EXE..R.....CW.V.Y.~..... ..H..c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....C.C>.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.. ...\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o .n.F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Chrome Apps\YouTube.lnk	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Has command line arguments, Icon number=0, Archive, ctime=Tue Oct 3 09:48:42 2023, mtime=Wed Aug 21 14:54:26 2024, atime=Wed Sep 27 04:28:28 2023, length=1210144, window=hide
Category:	dropped
Size (bytes):	2683
Entropy (8bit):	3.9931625362861096
Encrypted:	false
SSDEEP:	48:8pdjwTDUUHHTidAKZdA1duT+ehOuTbbiZUk5OjqehOuTbLy+yT+:8fwHXST/TbxWOvTbLy7T
MD5:	84BE2F01BC3404EA7D219CB1946C621A
SHA1:	A8BC038D20F52D6414AE03C0B30B195932E78ECE
SHA-256:	3DF9B976206E631B6BE9F02B6ADE5182CC7AB765BC1C3AB867033D8091C78B66
SHA-512:	3E7B8AEE1DEC8A3ED2953027DE4C355DD87B75A194B59BA3D5B1166358AC82DC86D4C76F2327733AB2C4284D4159AA9B73BA8B7F41343FD51BB02368709C099
Malicious:	false
Reputation:	low
Preview:	L.....F.@.. ...$+.,.....7yf....N.Yr.... w.....1....P.O. .:i.....+00.../C:\.....1.....DWWn..PROGRA~1..t.....O.I.Y.~....B.....J.....SX.P.r.o.g.r.a.m. .F.i .l.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.1.....T.1.....CW.V..Google..>.....CW.V.Y.~....L.....p+j.G.o.o.g.l.e.....T.1.....CW.V..Chrome..>.....CW.V.Y.~....M..... .....8..C.h.r.o.m.e.....`.1.....CW.V..APPLIC~1..H.....CW.V.Y.~....."&.A.p.p.l.i.c.a.t.i.o.n.....n.2. w..;W.+ .CHROME~1.EXE..R.....CW.V.Y.~..... ..H..c.h.r.o.m.e._.p.r.o.x.y...e.x.e.....j.....-.....i.....C.C>.....C:\Program Files\Google\Chrome\Application\chrome_proxy.exe..S.....\.....\.....\.....\.....\.....\.....\.....\.. ...\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e._.p.r.o.x.y...e.x.e.*.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o .n.F

Chrome Cache Entry: 130	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	934
Entropy (8bit):	5.219757940393194
Encrypted:	false
SSDEEP:	24:t4l6nGWTJgMXLxu0IfOoD9FZt8Rz57ElRb:knNmxD9t8m
MD5:	D8F2F390483A075C9BB320FD8C2536F8
SHA1:	452044FB20DBABC7CAA1E28FAB69332AA2D4C9EC
SHA-256:	41F2B485D051C3FD0CE738A71CC5CC2E1F459F8BA4644716C20511258229B37F
SHA-512:	1099FD3A3EC86C4B56FF3F9232CF35D2624A06C632E154D5EDF5171CF27E96E8A4D1FAA8EC90E84C1C94DD602D6693631B7054910CF4FB0D8917DD7708E3DA7
Malicious:	false
Reputation:	low
URL:	http://https://cdn.slab.com/images/favicon-d8f2f390483a075c9bb320fd8c2536f8.svg?vsn=d
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="none" viewBox="0 0 16 16"><style>@media all and (max-width:33px){#b{display:none}}</style><g fill-rule="evenodd" clip-path="url(#a)" clip-rule="evenodd"><path fill="#50C5DC" d="M7.995 5.3h8V3.767c0-2.08-1.79-3.767-4-3.767H4.233c2.094.12 3.762 5.3 3.762 5.3Z"/><path fill="#FCB415" d="M8 8H0V3.91C0 1.75 1.79 0 4 0h7.762C9.668.125 7.986 1.823 7.986 3.901L8 8Z"/><path fill="#741448" d="M8.005 10.78h-8v1.533c0 2.08 1.79 3.767 4 3.767h7.762c-2.095-.12-3.762-5.3-3.762-5.3Z"/><path fill="#FF4143" d="M8 8h8v4.09c0 2.16-1.79 3.91-4 3.91H4.238c2.094-.125 3.776-1.823 3.776-3.901L8 8Z"/><path id="b" fill="#fff" d="M1.55 6.524h4.885v-.652H1.55v.652Zm0-1.486h4.885v-.652H1.55v.652Zm0-1.486h4.885V2.9H1.55v.652Zm7.98 6.6h4.885V9.5H9.53v.652Zm0 1.486h4.885v-.652H9.53v.652Zm0 1.486h4.885v-.652H9.53v.652Z"/></g><defs><clipPath id="a"><path fill="#fff" d="M0 0h16v16H0V0Z"/></clipPath></defs></svg>

Chrome Cache Entry: 131	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	105589
Entropy (8bit):	5.174631095894137

Encrypted:	false
SSDEEP:	768:MLMeCBCBkiC/MFRo43esRdLyWQL9XJYOLBOiDYdveR2CjRBKF2FTm7L/PTDFIls4:0CBNh/E1D82vnCjRBKFgTmbRFnOoh2
MD5:	40A94E273500AE9ED6FF9B655B288E32
SHA1:	7CE82667DC5F86AECC2B671C16C7C5F15FC87CAE
SHA-256:	800FEAD8C2B7E0423585FC50F1E6955F2DF6C67EDFA5322B9088DE40255B7BE3
SHA-512:	26EBF4C5331C431BE3BDB2E8305EE18499769136BA065502C7D1EA8F7788B94DF7FF548F2E7D378E3F1BBB2D2CD53911884C2A07D5166D827E5696F84F7965A7
Malicious:	false
Reputation:	low
URL:	http://https://cdn.segment.com/analytics.js/v1/QfBlWGugy5p510EIBmtx2y6XsqRIyNsq/analytics.min.js
Preview:	!function(){var t,e,n,r,i={8878:function(t,e,n){"use strict";var r=this&&this.__importDefault||function(t){return t&&t.__esModule?t:{default:t}};Object.defineProperty(e,"__esModule",{value:!0});var i=r(n(325));function o(t,e){return function(){var n=this.traits(),r=this.properties?this.properties():{};return i.default(n,"address."+t)||i.default(n,t)||(e?i.default(n,"address."+e):null)||(e?i.default(n,e):null)||i.default(r,"address."+t)||i.default(r,t)||(e?i.default(r,"address."+e):null)||(e?i.default(r,e):null)}}e.default=function(t){t.zip=o("postalCode","zip"),t.country=o("country"),t.street=o("street"),t.state=o("state"),t.city=o("city"),t.region=o("region")}},4780:function(t,e,n){"use strict";var r=this&&this.__importDefault||function(t){return t&&t.__esModule?t:{default:t}};Object.defineProperty(e,"__esModule",{value:!0}),e.Alias=void 0;var i=r(n(1285)),o=n(9512);function s(t,e){o.Facade.call(this,t,e)}e.Alias=s,i.default(s,o.Facade),s.prototype.action=function(){return"alias"},s.p

Chrome Cache Entry: 132

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1818
Entropy (8bit):	4.623646989739716
Encrypted:	false
SSDEEP:	24:YybpIf4SJLKnxBYQmYXENhyGLR6bxghwWKGV2YcGtBoVhGr:YybpIf4mLUHYQmYXENVQ+DV2YcUB+hC
MD5:	10C9A9FDD67F69F62ECDBD1F3631FB8F
SHA1:	E6383ACD122FDF94D8907045BD57F087716F0CAD
SHA-256:	8F9C3DA5468B0DAB662A44679ABFFB63DE8D2DF3C0E2259FD2D59E713CAA8133
SHA-512:	ED73A75C7D0A03280490422E5DBFEA1220EAAAA880735DAFEDB2193C7E92DFB127FF1E4811C1A2753ECC29F5F361E704019C7E00A6C074359F84A6C01843AF14
Malicious:	false
Reputation:	low
Preview:	{"integrations":{"Segment.io":{"apiKey":"QfBlWGugy5p510EIBmtx2y6XsqRIyNsq","unbundledIntegrations":[],"addBundledMetadata":true,"maybeBundledConfigIds":{},"versionSettings":{"version":"4.4.7","componentTypes":["browser"]},"retryQueue":true}},"plan":{"track":{"__default":{"enabled":true,"integrations":{}}},"identify":{"__default":{"enabled":true},"clearbit_company_category_industry_group":{"enabled":true},"clearbit_company_category_sector":{"enabled":true},"clearbit_company_description":{"enabled":true},"clearbit_company_domain":{"enabled":true},"clearbit_company_domain_aliases":{"enabled":true},"clearbit_company_geo_city":{"enabled":true},"clearbit_company_geo_state":{"enabled":true},"clearbit_company_geo_state_code":{"enabled":true},"clearbit_company_geo_sub_premise":{"enabled":true},"clearbit_company_legal_name":{"enabled":true},"clearbit_company_metrics_market_cap":{"enabled":true},"clearbit_company_site_phone_numbers":{"enabled":true},"clearbit_company_time_zone":{"enabled":true},"

Chrome Cache Entry: 133

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	RIFF (little-endian) data, Web/P image
Category:	downloaded
Size (bytes):	2508
Entropy (8bit):	7.891354380364917
Encrypted:	false
SSDEEP:	48:/gott4QPDkQ5qpak+NSWeGcrPdUHx6pWQfvp1nrEpYWF:/git5PDk8qpjO7eGcjdUHx6pWevTrEzF
MD5:	DDDECB9D6172A6A3907B4C68B55CB904
SHA1:	2353AB8F44835CED58097BBD0302734C0E8CF093
SHA-256:	E6651253B2E40B62ACF41D7B1ED46119DABB7A3444D3ED3FBC99740094AAB07A
SHA-512:	49A3882D77FB2A6313EF92FCA6EDEE9333B20DC5142F0ECEE923D0B9ED92D472CB17345437501AA52E78FC4F55FC7DFBE7ACD24906BED83CA5A0C0A0927BD34C
Malicious:	false
Reputation:	low
URL:	http://https://cdn.slab.com/images/favicon-4cd04a6c3329f76935c9b946f0cc2902.png?vsn=d
Preview:	RIFF....WEBPVP8L..../..c."..../r.[..l...yVU.....>}|....f.(i6.\.M..$.V.....)7.....2cg.aN..03...p. ...c...mo...T.A.....K..u.V...[..T.w.....+,.....y,.R.+N....M.Lur.M.iw..\d.....4....B...X...c.F.H $...._...m....@~.X...`.j7.!...=...Dh.J.....8..\..e8 ].g....)>.U...t.L....C.B.)..._..y.).z.W....xL....7.r...`"uMV\..-r?../.k.%.3..8W...)...P...m....'7.8.@E.:l..B%...O.j..A.tx....n1.'.|.IK$....1.H.[.T{S...*.j.J.....u..g.z...n.E@ ....1.?.-.Mt..R.)t.'.=.H.....);.Wo....GQ.Z(..?N.....D....=U+S.z>k.#_..o.....=.....a.?x.y{.B.|.K....x.....F..wU.."Z.?..C(/.eD.(z..J~.D)...@E...z^..E..V1".0^..P..+..Y.p.?Fa%.[....Fj.....y.w..]........1.T."...P.....p.........S.....i.(EF.%..y..S)J.$.-M...&.FO.o.5.fx.l.R45...P....9. .....c.w..0..W&..".z.4..o!.PX.....L....F.....}[E....#..b.5..x.J&....#....)p...y.:.bH6.D.<.1E.L..g.N.r.....L.1.....4s.C.n.......ahj./...t.T....HN..u..A....Q.2.Gd~.".6...S<.m.j.l.C....!....t8=..I.CA.....;....f,.-t'...1..]v..

Chrome Cache Entry: 134

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators

Category:	dropped
Size (bytes):	105589
Entropy (8bit):	5.174631095894137
Encrypted:	false
SSDEEP:	768:MLMeCBCBkiC/MFRo43esRdLyWQL9XJYOLBOiDYdveR2CjRBKF2FTm7L/PTDFIls4:0CBNh/E1D82vnCjRBKFgTmbRFnOoh2
MD5:	40A94E273500AE9ED6FF9B655B288E32
SHA1:	7CE82667DC5F86AECC2B671C16C7C5F15FC87CAE
SHA-256:	800FEAD8C2B7E0423585FC50F1E6955F2DF6C67EDFA5322B9088DE40255B7BE3
SHA-512:	26EBF4C5331C431BE3BDB2E8305EE18499769136BA065502C7D1EA8F7788B94DF7FF548F2E7D378E3F1BBB2D2CD53911884C2A07D5166D827E5696F84F7965A
Malicious:	false
Reputation:	low
Preview:	!function(){var t,e,n,r,i={8878:function(t,e,n){"use strict";var r=this&&this.__importDefault||function(t){return t&&t.__esModule?t:{default:t}};Object.defineProperty(e,"__esModule",{value:!0});var i=r(n(325));function o(t,e){return function(){var n=this.traits(),r=this.properties?this.properties():{};return i.default(n,"address."+t)||i.default(n,t)||(e?i.default(n,"address."+e):null)||(e?i.default(n,e):null)||i.default(r,"address."+t)||i.default(r,t)||(e?i.default(r,"address."+e):null)||(e?i.default(r,e):null)}}e.default=function(t){t.zip=o("postalCode","zip"),t.country=o("country"),t.street=o("street"),t.state=o("state"),t.city=o("city"),t.region=o("region")}},4780:function(t,e,n){"use strict";var r=this&&this.__importDefault||function(t){return t&&t.__esModule?t:{default:t}};Object.defineProperty(e,"__esModule",{value:!0}),e.Alias=void 0;var i=r(n(1285)),o=n(9512);function s(t,e){o.Facade.call(this,t,e)}e.Alias=s,i.default(s,o.Facade),s.prototype.action=function(){return"alias"},s.p

Chrome Cache Entry: 135

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (49024)
Category:	downloaded
Size (bytes):	323716
Entropy (8bit):	4.94111177998248
Encrypted:	false
SSDEEP:	1536:N74M4bTbOE1EFcwyYbg/0jsTgTYH7ehuQk3/iV71O7/zH9gaznQ1RQuf//7ZNv7r:NDfOOcPYbg/0jsTgTYH+
MD5:	30C3092EA9AF23A639832F0B52D33537
SHA1:	7B4D4E7D43824FF76D87B8387937D45C2A1AA866
SHA-256:	0EA8C6BB7E760B1E591744C2A527F0F5B27CD06577B6212824EC05B9ADE7A41E
SHA-512:	8782561D6FC07F8480EFC3A84BEE32E5E0DAB610F9D4C75B03B8D78A76C083DFA23252EB8F6643C48F67214257F299B35C19A050AB704189E97375E9D4CABE7
Malicious:	false
Reputation:	low
URL:	http://https://cdn.slab.com/bundles/css/internal-30c3092ea9af23a639832f0b52d33537.css?vsn=d
Preview:	/*!. * Quill Editor v2.0.2. * https://quilljs.com. * Copyright (c) 2017-2024, Slab. * Copyright (c) 2014, Jason Chen. * Copyright (c) 2013, salesforce.com. */.ql-container{box-sizing:border-box;font-family:Helvetica,Arial,sans-serif;font-size:13px;height:100%;margin:0;position:relative}.ql-container.ql-disabled .ql-tooltip{visibility:hidden}.ql-container:not(.ql-disabled) li[data-list=checked]>.ql-ui,.ql-container:not(.ql-disabled) li[data-list=unchecked]>.ql-ui{cursor:pointer}.ql-clipboard{height:1px;left:-100000px;overflow-y:hidden;position:absolute;top:50%}.ql-clipboard p{margin:0;padding:0}.ql-editor{word-wrap:break-word;box-sizing:border-box;counter-reset:list-0 list-1 list-2 list-3 list-4 list-5 list-6 list-7 list-8 list-9;height:100%;line-height:1.42;outline:none;overflow-y:auto;padding:12px 15px;tab-size:4;-moz-tab-size:4;text-align:left;white-space:pre-wrap}.ql-editor>*{cursor:text}.ql-editor blockquote,.ql-editor h1,.ql-editor h2,.ql-editor h3,.ql-editor h4,.ql-editor h5,.ql-

Chrome Cache Entry: 136

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	934
Entropy (8bit):	5.219757940393194
Encrypted:	false
SSDEEP:	24:t4l6nGWTJgMXLxu0IfOoD9FZt8Rz57ElRb:knNmxD9t8m
MD5:	D8F2F390483A075C9BB320FD8C2536F8
SHA1:	452044FB20DBABC7CAA1E28FAB69332AA2D4C9EC
SHA-256:	41F2B485D051C3FD0CE738A71CC5CC2E1F459F8BA4644716C20511258229B37F
SHA-512:	1099FD3A3EC86C4B56FF3F9232CF35D2624A06C632E154D5EDF5171CF27E96E8A4D1FAA8EC90E84C1C94DD602D6693631B7054910CF4FB0D8917DD7708E3DA7
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="none" viewBox="0 0 16 16"><style>@media all and (max-width:33px){#b{display:none}}</style><g fill-rule="evenodd" clip-path="url(#a)" clip-rule="evenodd"><path fill="#50C5DC" d="M7.995 5.3h8V3.767c0-2.08-1.79-3.767-4-3.767H4.233c2.094.12 3.762 5.3 3.762 5.3Z"/><path fill="#FCB415" d="M8 8H0V3.91C0 1.75 1.79 0 4 0h7.762C9.668.125 7.986 1.823 7.986 3.901L8 8Z"/><path fill="#741448" d="M8.005 10.78h-8v1.533c0 2.08 1.79 3.767 4 3.767h7.762c-2.095-.12-3.762-5.3-3.762-5.3Z"/><path fill="#FF4143" d="M8 8h8v4.09c0 2.16-1.79 3.91-4 3.91H4.238c2.094-.125 3.776-1.823 3.776-3.901L8 8Z"/><path id="b" fill="#fff" d="M1.55 6.524h4.885v-.652H1.55v.652Zm0-1.486h4.885v-.652H1.55v.652Zm0-1.486h4.885V2.9H1.55v.652Zm7.98 6.6h4.885V9.5H9.53v.652Zm0 1.486h4.885v-.652H9.53v.652Zm0 1.486h4.885v-.652H9.53v.652Z"/></g><defs><clipPath id="a"><path fill="#fff" d="M0 0h16v16H0V0Z"/></clipPath></defs></svg>

Chrome Cache Entry: 137

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4582
Entropy (8bit):	7.580455544298349
Encrypted:	false
SSDEEP:	96:5Zqb9yMYtu9nExThtfle62gNJCJCJF4SrNU469BA7czad36eC/19Frq/0g:5072HDsgNJCJCJ2uS4xsad3pqlK
MD5:	D9B7C7BF3CCC45AC1282AEF867FE71F8
SHA1:	860A1A0BDE3B6461DFDA47CFB2A0FC3981C26908
SHA-256:	BC0CE6FD008D204A18443D677A940876A9215AF55206C8FD09907ECDF9DEE57A
SHA-512:	1E30DD6A7B4EFCBA5F63C27D59419FBDD640289B5E19F61C1CF5A85BE8B699D4BE2B90D1011AE2B2616668C3AA11D2B5D611283D5A75CEA876B1A8FE82D67 5A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....6.....sRGB.....gAMA.....a.....IDATx...O.a..q...\g";q.....C.....Xd....S..Jl.....G.7.(2.H..=....#-i)..>.'..<.<.....5.R...laz...#}j.K'.#sZ4...a..F....E.....=...EU .M.\eEe.^....j.ZR.k5e.....G....6.@.73f..fV.i.9o.4...[....~X.l@....c.N..[.'..A8<.7...I.!A..L..I.P7....*d..I....sK.z.B..$.....Q#.....3a....d.../k:n.@....Ylu.d.....~/.6&Z.9Sa.E....t3e ..Co..!...3..&...:.4..._O.Ah\.&.K..b7m$W..@..z..B.4..A8...):l.....hs.....l....l..g...%H.. ....o..AB...`..EVU..u.~.}...M..p|.t./..t.1..q..s...K....\....`x4...S.9XkQ....K..p...9.U..(....#..L# C,..@..e.`...nX...i.....Ws..q7.F.Q.....<...G[..N*...XY...VV.M..J.YY...4.F.....n.[V..V..].;..;.6...K.EN.....]p.T..eE...6...$8\'<....f.r.Ds.!Bx..... <@.....B.....B...@.%..... ..x...'2.7.i..o.cl..%.....'.B. Hs.M.....i*....%.P.....n..7.....&,]X..g....R..T.O..M.\.Q.c.L.....CR....'.s..&.%.....MwgY..C..~KS...f.....V.sU.....:.L....~.d$.u.<>.Q..WdV.U."s...7.4/..{...

Chrome Cache Entry: 138	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	243783
Entropy (8bit):	6.003697934864325
Encrypted:	false
SSDEEP:	6144:cooVEoGYKvtQM3OlFlJZkEA6oJMeGMHhxsl:loVJi1327rA67eGMHhxsl
MD5:	A457DD5957962BB27CC0DBD618D8643F
SHA1:	499531ED07A60EA8479D7B696842E0924D8F0290
SHA-256:	A1DE959DB6C7EDA1A65EAD13358876DD2243958E4B1EF1707CA66EA0D73DDE75
SHA-512:	FE77EAE365EBC8FE86B00DCB9E3F79D4629C622BA607D79DC31CE39A2CC3996006FDD613318B48D2E6D3EA96D0D243C934AFB3BFAD05724CACED02FCC99A 555A
Malicious:	false
Reputation:	low
URL:	http://https://cdn.slab.com/bundles/css/fonts/web-1982fc99f3624125665d704ac0753574.css?vsn=d
Preview:	@font-face{font-family:IBM Plex Mono;font-style:normal;font-weight:450;src:url(data:application/font-woff;base64,d09GRgABAAAAAMg4ABEAAAABuowAAQABAAAAA AAAAAAAAAAAAAAAAAAAAABHREVGAAABgAAAAGsAAACCG2YbSUdQT1MAAAHsAAACfgAABR4nQVLhR1NVQgAABGwAAAU7AAAJujFugWpPUy8yAAA JqAAAAFoAAABgiwFprmNtYXAAAAoEAAAHMgAACmajlxLpY3Z0IAAAETgAAABAAAAAQA5kAspmcGdtAAAReAAAAQIAAAFzBlmcN2dhc3AAABJ8AAAAEAAAABA AGAAhZ2x5ZgAAEowAAJieAAFhyAGY18loZWFkAACrLAAAADYAAAA2DV0Q9GhoZWEAAKtkAAAAIQAAACQFfQONaG10eAAAq4gAAANqAAANUF7pxURsb2NhAAC u9AAABp8AAAaqAy2oEm1heHAAALWUAAAAIAAAACAFigNPbmFtZQAAtbQAAARxAAAJfZUmD65wb3N0AAC6KAAADRQAABwPBAFLQnByZXAAAMc8A AAA+gAAAbSaC0GmeJwlyjEKg1AQRdH7Zn4ZkBBwAyEgWNtYpBL7/F1ItuDmBPeQJn3AVeSBc+HAg0HAhfOCG4UGcWW0T2bvxRXervB1UihsI3+qU2d79baq2 lWr3bTZXbs9dKD4xI/INu9kPnKwU77IP+zxDtgAeJy9lD9MU1EUxr/7bvmnaLEBglpNrSKtrYXSFqWQSBSYukgYXYij6EA6KCEOisY0xjAYBuNgMDEODQNxM AwGEuJgHAiDcSAMpoPpYBwMgyHB7359CouLgzk5v/u9+86997zz7r0wAA7gMqZhh0cL42i9fmdqEpHJieItJBHgW+zuwkXtabNPe7A3J6ZuoFWMiEk/Wm//qgNcN4RjiPp 9kVprUn5bqrV2nP7QzjG

Chrome Cache Entry: 139	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (12829)
Category:	downloaded
Size (bytes):	17947
Entropy (8bit):	5.364903778791486
Encrypted:	false
SSDEEP:	384:PSojr7/rwW61sgHm5ZEeKKovF0PupupStdVo5r3dNhApRHyYFBzjdRkdrII+YxM3:LrgHm5ZETKoSPupkSjVo58RHy8zjdRkZ
MD5:	1F33DD9D80DB30E704948B9204383F74
SHA1:	7568CAD45B5B7C978FACCC65DDD5B09B64849028
SHA-256:	E034A3CA6A7FD273FDAC9C2015D7C26B8C0F887E97D3484D088B5E321A49CC34
SHA-512:	A7DB59F0A7E576CF94072A4E061C50460C2C1C830F44834A0F560610CD6ADCB9A435B0950C2B49C27D15B4FEFCB8A90BA0E3D4AFA27FC06186021DCE74B0B6 CE
Malicious:	false
Reputation:	low
URL:	http://https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGIslMBUruogrHIjh

Preview:	<!DOCTYPE html>.<html lang="en">.<head>. <meta charset="utf-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge">. <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no, viewport-fit=cover">. <meta name="slack-app-id" content="A4TSF7SR5">..<title>Slab - Your Team's Long Term Memory</title>.. <meta name="robots" content="noindex, nofollow">.... <meta property="description" content="Slab is a modern wiki with thoughtful UX, smart search, and integrations that helps your team find answers faster.">. <meta property="og:type" content="website">. <meta property="og:title" content="Slab - Your Team's Long Term Memory">. <meta property="og:url" content="https://slab.com/">. <meta property="og:description" content="Slab is a modern wiki with thoughtful UX, smart search, and integrations that helps your team find answers faster.">. <meta name="twitter:title" content="Slab - Your Team's Long Term Memory">. <meta name="twitter:description

Chrome Cache Entry: 140

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	1818
Entropy (8bit):	4.623646989739716
Encrypted:	false
SSDEEP:	24:YybpIf4SJLKnxBYQmYXENhyGLR6bxghwWKGV2YcGtBoVhGr:YybpIf4mLUHYQmYXENVQ+DV2YcUB+hC
MD5:	10C9A9FDD67F69F62ECDBD1F3631FB8F
SHA1:	E6383ACD122FDF94D8907045BD57F087716F0CAD
SHA-256:	8F9C3DA5468B0DAB662A44679ABFFB63DE8D2DF3C0E2259FD2D59E713CAA8133
SHA-512:	ED73A75C7D0A03280490422E5DBFEA1220EAAAA880735DAFEDB2193C7E92DFB127FF1E4811C1A2753ECC29F5F361E704019C7E00A6C074359F84A6C01843AF14
Malicious:	false
Reputation:	low
URL:	http://https://cdn.segment.com/v1/projects/QfBlWGugy5p510EIBmtx2y6XsqRIyNsq/settings
Preview:	{"integrations":{"Segment.io":{"apiKey":"QfBlWGugy5p510EIBmtx2y6XsqRIyNsq","unbundledIntegrations":[],"addBundledMetadata":true,"maybeBundledConfigIds":{},"versionSettings":{"version":"4.4.7","componentTypes":["browser"]},"retryQueue":true}},"plan":{"track":{"__default":{"enabled":true,"integrations":{}}},"identify":{"__default":{"enabled":true},"clearbit_company_category_industry_group":{"enabled":true},"clearbit_company_category_sector":{"enabled":true},"clearbit_company_description":{"enabled":true},"clearbit_company_domain":{"enabled":true},"clearbit_company_domain_aliases":{"enabled":true},"clearbit_company_geo_city":{"enabled":true},"clearbit_company_geo_state":{"enabled":true},"clearbit_company_geo_state_code":{"enabled":true},"clearbit_company_geo_sub_premise":{"enabled":true},"clearbit_company_legal_name":{"enabled":true},"clearbit_company_metrics_market_cap":{"enabled":true},"clearbit_company_site_phone_numbers":{"enabled":true},"clearbit_company_time_zone":{"enabled":true},"

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 62

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 21, 2024 17:54:15.135734081 CEST	49674	443	192.168.2.5	23.1.237.91

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 21, 2024 17:54:15.135883093 CEST	49675	443	192.168.2.5	23.1.237.91
Aug 21, 2024 17:54:15.260772943 CEST	49673	443	192.168.2.5	23.1.237.91
Aug 21, 2024 17:54:24.854571104 CEST	49674	443	192.168.2.5	23.1.237.91
Aug 21, 2024 17:54:24.916949034 CEST	49675	443	192.168.2.5	23.1.237.91
Aug 21, 2024 17:54:24.916960001 CEST	49673	443	192.168.2.5	23.1.237.91
Aug 21, 2024 17:54:26.763087034 CEST	443	49703	23.1.237.91	192.168.2.5
Aug 21, 2024 17:54:26.763171911 CEST	49703	443	192.168.2.5	23.1.237.91
Aug 21, 2024 17:54:26.962403059 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:26.962445974 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:26.962532997 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:26.962838888 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:26.962855101 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:27.263835907 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.263880968 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.264049053 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.264059067 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.264081001 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.264139891 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.264353991 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.264369011 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.264554024 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.264570951 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.626552105 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:27.658689976 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:27.658723116 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:27.659646034 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:27.659717083 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:27.667748928 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:27.667819977 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:27.722743034 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:27.722765923 CEST	443	49709	216.58.206.68	192.168.2.5
Aug 21, 2024 17:54:27.732021093 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.733549118 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.762630939 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.762665033 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.762770891 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.762804985 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.763951063 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.764019966 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.764102936 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.764158010 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.768332958 CEST	49709	443	192.168.2.5	216.58.206.68
Aug 21, 2024 17:54:27.777909994 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.778032064 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.778481960 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.778491020 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.778661966 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.778831959 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.827420950 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.827444077 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:27.827465057 CEST	443	49711	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:27.876184940 CEST	49711	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.434458971 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434509039 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434540987 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434556007 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.434573889 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434585094 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434626102 CEST	49710	443	192.168.2.5	104.17.234.61

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 21, 2024 17:54:28.434628963 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434638023 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434678078 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.434679031 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434705973 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434724092 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.434724092 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434734106 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.434768915 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.441201925 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.441248894 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.441261053 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.441293001 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.441334963 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.441339016 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.441374063 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.441414118 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.571317911 CEST	49710	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.571352005 CEST	443	49710	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.582350969 CEST	49714	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.582401037 CEST	443	49714	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.582468987 CEST	49714	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.582998037 CEST	49715	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.583034039 CEST	443	49715	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.583091974 CEST	49715	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.583903074 CEST	49715	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.583920002 CEST	443	49715	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:28.584379911 CEST	49714	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:28.584395885 CEST	443	49714	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.074428082 CEST	443	49714	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.075120926 CEST	49714	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:29.075151920 CEST	443	49714	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.078380108 CEST	443	49714	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.078500986 CEST	49714	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:29.078978062 CEST	443	49715	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.079914093 CEST	49715	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:29.079976082 CEST	443	49715	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.080435038 CEST	49714	443	192.168.2.5	104.17.234.61
Aug 21, 2024 17:54:29.080591917 CEST	443	49714	104.17.234.61	192.168.2.5
Aug 21, 2024 17:54:29.080899954 CEST	443	49715	104.17.234.61	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 21, 2024 17:54:25.542031050 CEST	53	59156	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:25.566292048 CEST	53	52087	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:26.594770908 CEST	53	65099	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:26.954175949 CEST	62989	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:26.954333067 CEST	58512	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:26.961210966 CEST	53	62989	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:26.961481094 CEST	53	58512	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:27.225497007 CEST	53118	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:27.225908995 CEST	55724	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:27.236888885 CEST	53	55724	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:27.244704008 CEST	53	53118	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:28.567809105 CEST	62363	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:28.568845987 CEST	61345	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:28.577228069 CEST	53	62363	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:28.579350948 CEST	53	61345	1.1.1.1	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 21, 2024 17:54:29.678050995 CEST	62094	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:29.679055929 CEST	61466	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:29.685241938 CEST	53	62094	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:29.686569929 CEST	53	61466	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:31.549952984 CEST	62814	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:31.551440001 CEST	61795	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:31.557651997 CEST	53	62814	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:31.558768988 CEST	53	61795	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:33.145669937 CEST	52360	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:33.146616936 CEST	60764	53	192.168.2.5	1.1.1.1
Aug 21, 2024 17:54:33.154772997 CEST	53	52360	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:33.157633066 CEST	53	60764	1.1.1.1	192.168.2.5
Aug 21, 2024 17:54:43.633306026 CEST	53	49248	1.1.1.1	192.168.2.5
Aug 21, 2024 17:55:02.414625883 CEST	53	57901	1.1.1.1	192.168.2.5
Aug 21, 2024 17:55:07.478771925 CEST	53	61211	1.1.1.1	192.168.2.5
Aug 21, 2024 17:55:24.951653957 CEST	53	57096	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Aug 21, 2024 17:54:26.954175949 CEST	192.168.2.5	1.1.1.1	0xc82f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:26.954333067 CEST	192.168.2.5	1.1.1.1	0x2a5e	Standard query (0)	www.google.com	65	IN (0x0001)	false
Aug 21, 2024 17:54:27.225497007 CEST	192.168.2.5	1.1.1.1	0x7e44	Standard query (0)	zackboyer.slab.com	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:27.225908995 CEST	192.168.2.5	1.1.1.1	0x3786	Standard query (0)	zackboyer.slab.com	65	IN (0x0001)	false
Aug 21, 2024 17:54:28.567809105 CEST	192.168.2.5	1.1.1.1	0xebf4	Standard query (0)	cdn.slab.com	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:28.568845987 CEST	192.168.2.5	1.1.1.1	0x997d	Standard query (0)	cdn.slab.com	65	IN (0x0001)	false
Aug 21, 2024 17:54:29.678050995 CEST	192.168.2.5	1.1.1.1	0x6d35	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:29.679055929 CEST	192.168.2.5	1.1.1.1	0x43af	Standard query (0)	cdn.segment.com	65	IN (0x0001)	false
Aug 21, 2024 17:54:31.549952984 CEST	192.168.2.5	1.1.1.1	0x8b46	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:31.551440001 CEST	192.168.2.5	1.1.1.1	0x751c	Standard query (0)	cdn.segment.com	65	IN (0x0001)	false
Aug 21, 2024 17:54:33.145669937 CEST	192.168.2.5	1.1.1.1	0x478b	Standard query (0)	cdn.slab.com	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:33.146616936 CEST	192.168.2.5	1.1.1.1	0x51f0	Standard query (0)	cdn.slab.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Aug 21, 2024 17:54:26.961210966 CEST	1.1.1.1	192.168.2.5	0xc82f	No error (0)	www.google.com		216.58.206.68	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:26.961481094 CEST	1.1.1.1	192.168.2.5	0x2a5e	No error (0)	www.google.com			65	IN (0x0001)	false
Aug 21, 2024 17:54:27.236888885 CEST	1.1.1.1	192.168.2.5	0x3786	No error (0)	zackboyer.slab.com			65	IN (0x0001)	false
Aug 21, 2024 17:54:27.244704008 CEST	1.1.1.1	192.168.2.5	0x7e44	No error (0)	zackboyer.slab.com		104.17.234.61	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:27.244704008 CEST	1.1.1.1	192.168.2.5	0x7e44	No error (0)	zackboyer.slab.com		104.17.235.61	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:28.577228069 CEST	1.1.1.1	192.168.2.5	0xebf4	No error (0)	cdn.slab.com		104.17.234.61	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Aug 21, 2024 17:54:28.577228069 CEST	1.1.1.1	192.168.2.5	0xebf4	No error (0)	cdn.slab.com		104.17.235.61	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:28.579350948 CEST	1.1.1.1	192.168.2.5	0x997d	No error (0)	cdn.slab.com			65	IN (0x0001)	false
Aug 21, 2024 17:54:29.685241938 CEST	1.1.1.1	192.168.2.5	0x6d35	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Aug 21, 2024 17:54:29.685241938 CEST	1.1.1.1	192.168.2.5	0x6d35	No error (0)	d296je7bbdd650.cloudfront.net		108.157.152.187	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:29.686569929 CEST	1.1.1.1	192.168.2.5	0x43af	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Aug 21, 2024 17:54:31.557651997 CEST	1.1.1.1	192.168.2.5	0x8b46	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Aug 21, 2024 17:54:31.557651997 CEST	1.1.1.1	192.168.2.5	0x8b46	No error (0)	d296je7bbdd650.cloudfront.net		13.227.222.191	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:31.558768988 CEST	1.1.1.1	192.168.2.5	0x751c	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Aug 21, 2024 17:54:33.154772997 CEST	1.1.1.1	192.168.2.5	0x478b	No error (0)	cdn.slab.com		104.17.234.61	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:33.154772997 CEST	1.1.1.1	192.168.2.5	0x478b	No error (0)	cdn.slab.com		104.17.235.61	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:33.157633066 CEST	1.1.1.1	192.168.2.5	0x51f0	No error (0)	cdn.slab.com			65	IN (0x0001)	false
Aug 21, 2024 17:54:36.615546942 CEST	1.1.1.1	192.168.2.5	0x44ad	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Aug 21, 2024 17:54:36.615546942 CEST	1.1.1.1	192.168.2.5	0x44ad	No error (0)	fp2e7a.wpc.phicdn.net		192.229.221.95	A (IP address)	IN (0x0001)	false
Aug 21, 2024 17:54:50.638995886 CEST	1.1.1.1	192.168.2.5	0x3e03	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Aug 21, 2024 17:54:50.638995886 CEST	1.1.1.1	192.168.2.5	0x3e03	No error (0)	fp2e7a.wpc.phicdn.net		192.229.221.95	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- zackboyer.slab.com
- https:
  - cdn.slab.com
  - cdn.segment.com
- fs.microsoft.com
- slscr.update.microsoft.com

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: **1788**, Parent PID: **5752**

General

Target ID:	0
Start time:	11:54:16
Start date:	21/08/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank"
Imagebase:	0x7ff715980000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **2824**, Parent PID: **1788**

General

Target ID:	2
Start time:	11:54:21
Start date:	21/08/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2372 --field-trial-handle=2296,i,6196848232246346782,16876402020592985407,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff715980000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4912**, Parent PID: **5752**

General	
Target ID:	3
Start time:	11:54:26
Start date:	21/08/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" "https://zackboyer.slab.com/posts/secured-file-ezhtf1ae?shr=5-QTmmuoGlslMBUruogrHIjh"
Imagebase:	0x7ff715980000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly