ID: 800707
Cookbook: browseurl.jbs
Time: 18:29:12
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

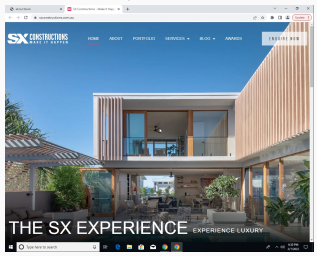
Windows Analysis Report

http://www.sxconstructions.com.au

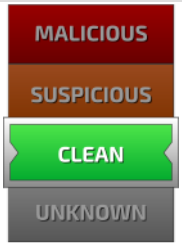
Overview

General Information

Sample URL:	http://www.sxconstructions.com.au
Analysis ID:	800707
Infos:	



Detection

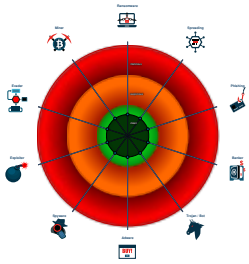


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 1768 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3480 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=1748 --field-trial-handle=1728,i,14009103719708538658,10673737706731050477,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4368 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.sxconstructions.com.au MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

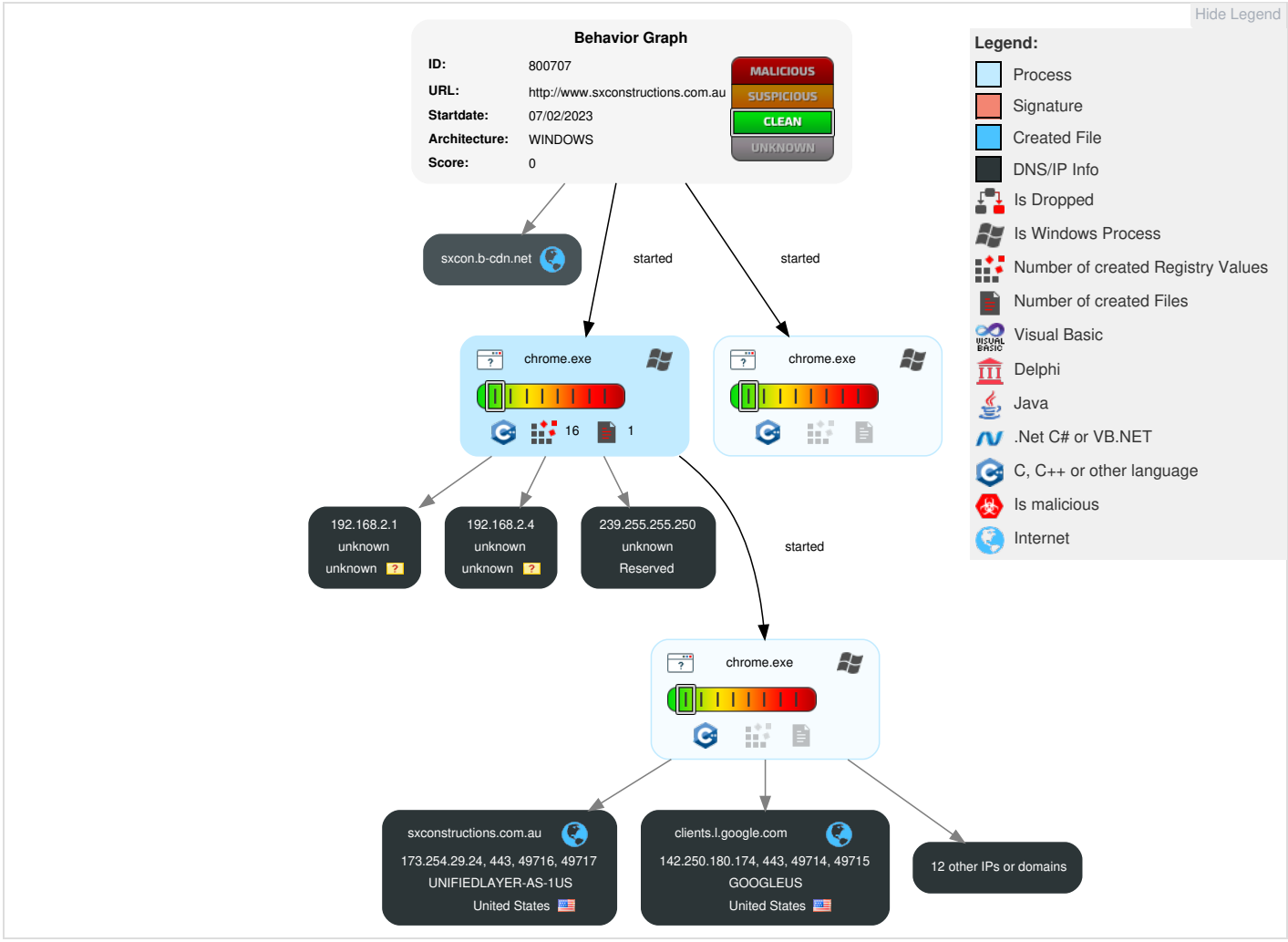
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

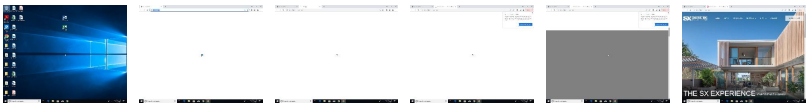
Behavior Graph

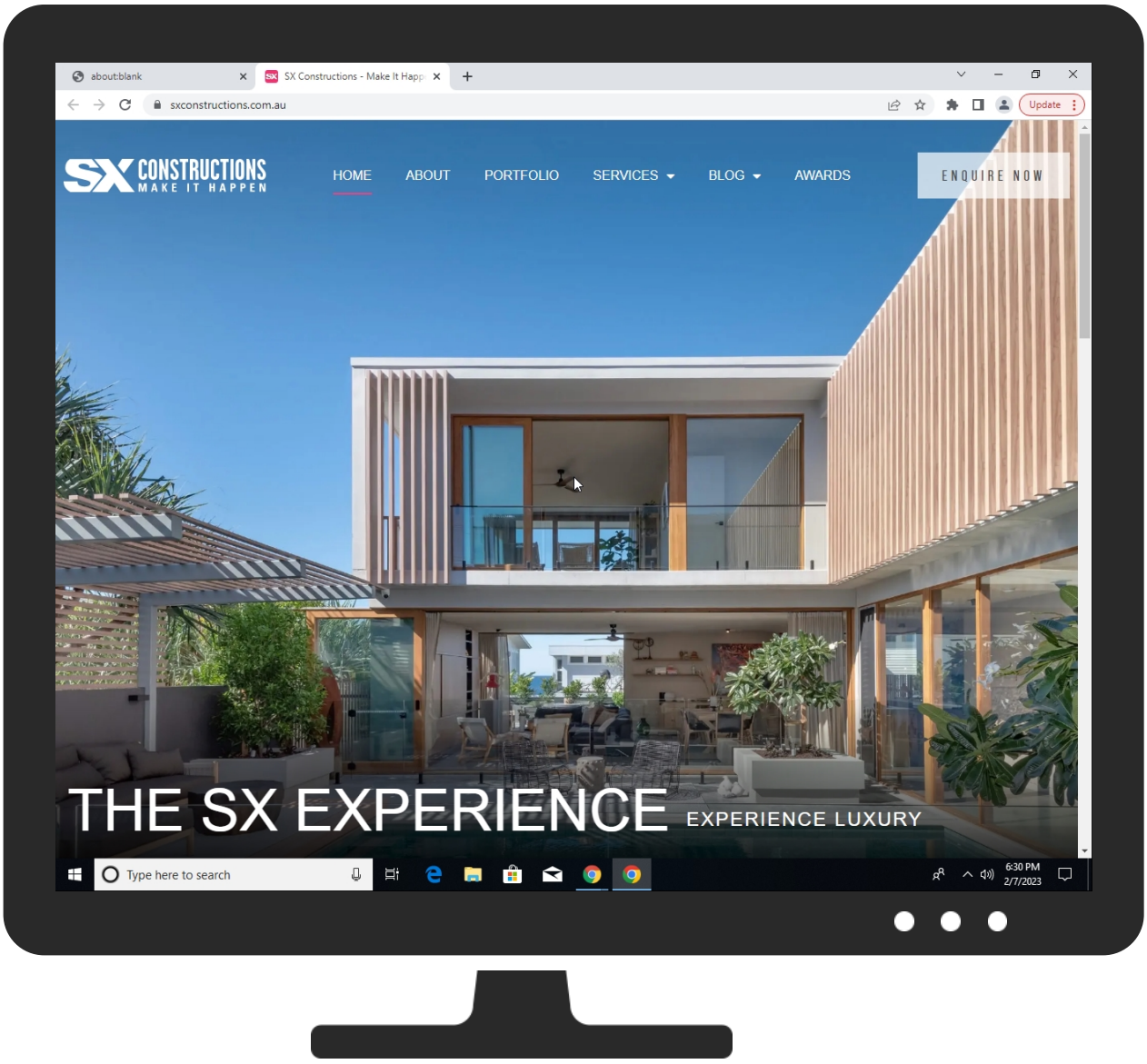


Screenshots

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://www.sxconstructions.com.au	1%	Virustotal		Browse
http://www.sxconstructions.com.au	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.sxconstructions.com.au/wp-content/uploads/2022/06/BG-scaled.jpg	0%	Avira URL Cloud	safe	
http://https://stats.wpmucdn.com/analytics.js	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://www.sxconstructions.com.au/wp-content/uploads/2022/06/Holiday-Style-Home34.jpg	0%	Avira URL Cloud	safe	
http://www.sxconstructions.com.au/	0%	Avira URL Cloud	safe	
http://https://stats1.wpmudev.com/track/?action_name=SX%20Constructions%20-%20Make%20It%20Happen&idsite=111120&rec=1&r=364363&h=18&m=30&s=20&url=https%3A%2F%2Fwww.sxconstructions.com.au%2F&_id=cd34969a54c0e9ab&_idts=1675823420&_idvc=1&_idn=1&_refts=0&_viewts=1675823420&send_image=1&cookie=1&res=1280x1024>_ms=844&pv_id=3yaHmO	0%	Avira URL Cloud	safe	
http://https://stats.wpmucdn.com/analytics.js	0%	Avira URL Cloud	safe	
http://https://www.sxconstructions.com.au/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sxconstructions.com.au	173.254.29.24	true	false		unknown
wpmu-stats.b-cdn.net	89.187.165.194	true	false		high
accounts.google.com	216.58.209.45	true	false		high
matomo-wpmudev-1288779782.us-east-2.elb.amazonaws.com	3.18.180.221	true	false		high
www.google.com	142.250.184.100	true	false		high
sxcon.b-cdn.net	89.187.165.194	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
stats.wpmucdn.com	unknown	unknown	false		unknown
use.typekit.net	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
www.sxconstructions.com.au	unknown	unknown	false		unknown
stats1.wpmudev.com	unknown	unknown	false		unknown

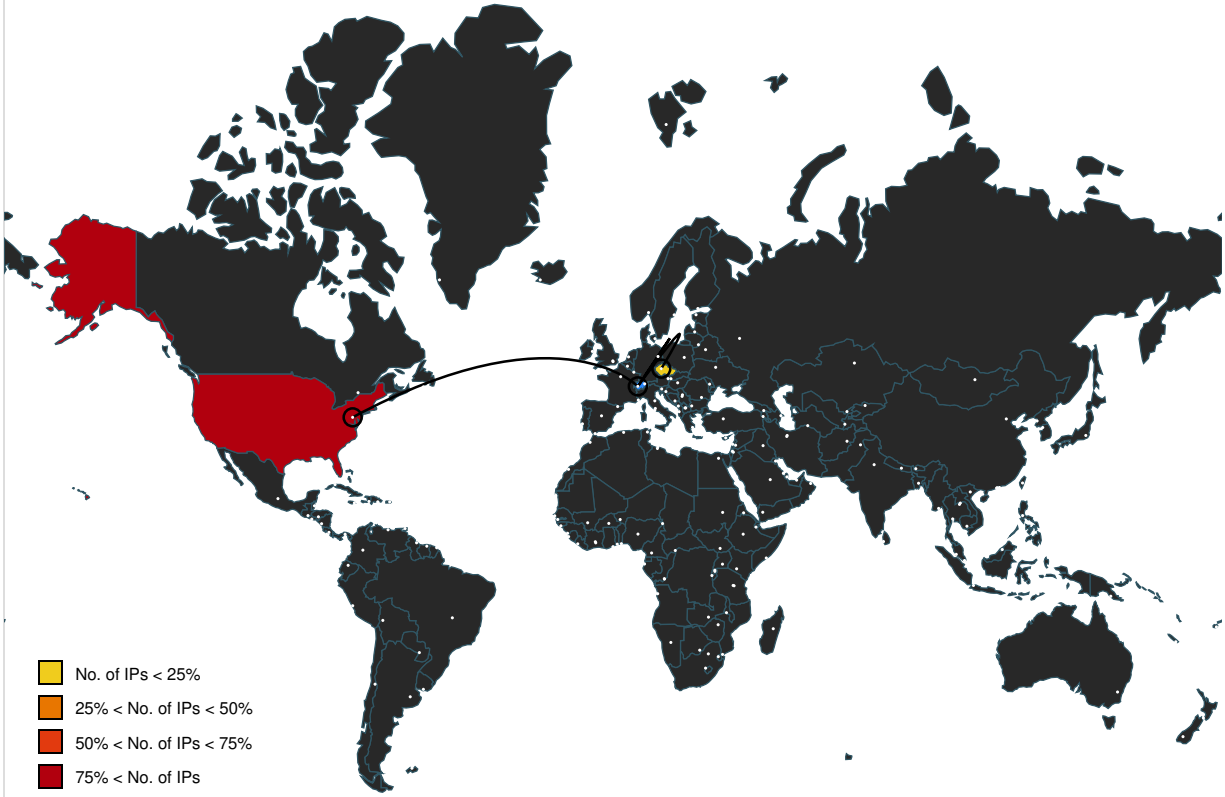
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sxcon.b-cdn.net/wp-includes/js/dist/hooks.min.js?ver=4169d3cf8e8d95a3d6d5	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2	false		high
http://https://stats.wpmucdn.com/analytics.js	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sxcon.b-cdn.net/wp-content/plugins/theplus_elementor_addon/assets/css/extra/fonts/iconsmind.woff	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/css/frontend-lite.min.css?ver=3.10.1	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/ui/slider.min.js?ver=1.13.2	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/theplus_elementor_addon/assets/css/extra/iconsmind.min.css?ver=5.0.10	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/css/frontend-lite.min.css?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/theplus_elementor_addon/assets/js/main/event-tracker/plus-event-tracker.min.js?ver=6.1.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=3.10.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6	false		high
http://https://www.sxconstructions.com.au/	false	• 0%, Virustotal, Browse	unknown
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/Logo.svg	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.9.0	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/cropped-Favicon4-32x32.png	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/wp-fastest-cache-premium/pro/images/blank.gif	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/jquery.ui.touch-punch.js?ver=0.2.2	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/font-awesome/webfonts/fa-brands-400.woff2	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/Group-155_LR-1024x484.jpg	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/elementor/css/post-6.css?ver=1673842299	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/lib/smartmenus/jquery.smartmenus.min.js?ver=1.0.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/js/webpack-pro.runtime.min.js?ver=3.10.1	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/elementor/css/post-1022.css?ver=1673842301	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/SX_Seafarer_015_WR.jpg	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/eicons/css/elementor-icons.min.css?ver=5.17.0	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/theplus-addons/theplus-post-9.min.css?ver=1673842300	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/font-awesome/css/solid.min.css?ver=5.15.3	false		high
http://https://www.sxconstructions.com.au/wp-content/uploads/2022/06/BG-scaled.jpg	false	• Avira URL Cloud: safe	unknown
http://https://sxcon.b-cdn.net/wp-content/uploads/elementor/css/post-7563.css?ver=1673842301	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/SX2.jpg	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/Holiday-Style-Home-1-1024x683.jpg	false		high
http://https://sxcon.b-cdn.net/wp-includes/css/dist/block-library/style.min.css?ver=6.1.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/css/widget-icon-list.min.css	false		high
http://https://sxcon.b-cdn.net/wp-content/themes/hello-elementor/theme.min.css?ver=2.6.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/js/preloaded-elements-handlers.min.js?ver=3.10.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets//lib/instant-page/instant-page.min.js?ver=3.10.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.10.0	false		high
http://https://www.sxconstructions.com.au/	false	• 0%, Virustotal, Browse	unknown
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/ui/draggable.min.js?ver=1.13.2	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/elementor/css/post-1017.css?ver=1673842301	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/elementor/css/global.css?ver=1673842300	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/js/page-transitions.min.js?ver=3.10.1	false		high
http://https://www.sxconstructions.com.au/wp-content/uploads/2022/06/Holiday-Style-Home34.jpg	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/js/preloaded-modules.min.js?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/theplus_elementor_addon/assets/js/main/section-column-link/plus-section-column-link.min.js?ver=6.1.1	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/css/widget-nav-menu.min.css	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/dist/i18n.min.js?ver=9e794f35a71bb98672ae	false		high
http://www.sxconstructions.com.au/	false	• Avira URL Cloud: safe	unknown
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/font-awesome/css/brands.min.css?ver=5.15.3	false		high
http://https://sxcon.b-cdn.net/wp-includes/css/classic-themes.min.css?ver=1	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/cropped-Favicon4-192x192.png	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/elementor/css/post-9.css?ver=1673842300	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/animations/animations.min.css?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/ui/mouse.min.js?ver=1.13.2	false		high
http://https://stats1.wpmudev.com/track/?action_name=SX%20Constructions%20-%20Make%20It%20Happen&idsite=111120&rec=1&r=364363&h=18&m=30&s=20&url=https%3A%2F%2Fwww.sxconstructions.com.au%2F&_id=cd34969a54c0e9ab&_idts=1675823420&_idvc=1&_idn=1&_refts=0&_viewts=1675823420&send_image=1&cookie=1&res=1280x1024>_ms=844&pv_id=3yaHmO	false	• Avira URL Cloud: safe	unknown
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/font-awesome/css/fontawesome.min.css?ver=5.15.3	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/css/frontend-legacy.min.css?ver=3.10.0	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/font-awesome/webfonts/fa-solid-900.woff2	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor/assets/lib/eicons/fonts/eicons.woff2?5.17.0	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/40-683x1024.jpg	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/jquery.min.js?ver=3.6.1	false		high
http://https://sxcon.b-cdn.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	false		high
http://https://sxcon.b-cdn.net/wp-content/uploads/2022/06/logo-housing-industry-association-member3-2-1024x156.png	false		high
http://https://sxcon.b-cdn.net/wp-content/themes/hello-elementor/style.min.css?ver=2.6.1	false		high
http://https://sxcon.b-cdn.net/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=3.10.1	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
173.254.29.24	sxconstructions.com.au	United States		46606	UNIFIEDLAYER-AS-1US	false
3.18.180.221	matomo-wpmudev-1288779782.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
89.187.165.194	wpmu-stats.b-cdn.net	Czech Republic		60068	CDN77GB	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800707
Start date and time:	2023-02-07 18:29:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.sxconstructions.com.au
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
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:	CLEAN
Classification:	clean0.win@24/0@10/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www.sxconstructions.com.au/#content

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 142.251.209.42, 216.58.209.42, 142.250.184.74, 142.250.184.106, 142.250.180.138, 142.250.180.170, 142.251.209.10, 142.250.184.67, 173.222.108.216, 173.222.108.232, 173.222.108.192, 80.67.82.195, 142.250.180.168, 142.250.184.110, 142.250.180.163
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, content-autofill.googleapis.com, fonts.gstatic.com, clientservices.googleapis.com, a1874.dscg1.akamai.net, p.typekit.net-stls-v3.edgesuite.net, maps.googleapis.com, edgedl.me.gvt1.com, use-stls.adobe.com.edgesuite.net, www.googletagmanager.com, update.googleapis.com, a1988.dscg1.akamai.net, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

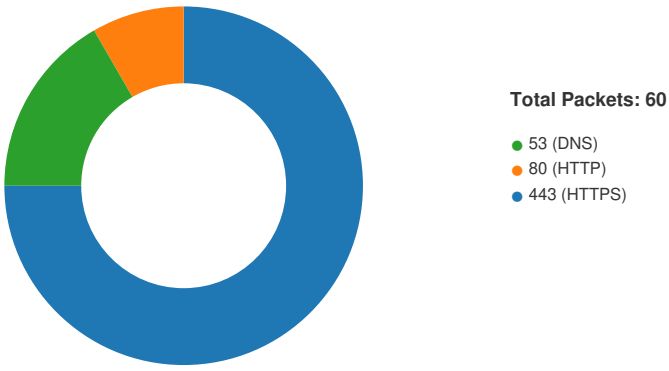
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:30:15.304320097 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:15.304363012 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:15.304447889 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:15.573915005 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:15.573981047 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:15.574074030 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:15.824090958 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:15.824162960 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:15.824265003 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:15.827769995 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:15.827831030 CET	443	49715	142.250.180.174	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:30:15.827933073 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:15.832783937 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:15.832844973 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:15.833044052 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:15.833080053 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:15.833367109 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:15.833383083 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:15.833525896 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:15.833575010 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:15.938368082 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:15.971324921 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:15.984153986 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:15.989535093 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.031857967 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.042156935 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.043900967 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.043911934 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.078847885 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.078885078 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.079495907 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.079534054 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.079646111 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.079725981 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.080980062 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.081017971 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.081082106 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.081115007 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.081139088 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.091860056 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.091893911 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.092004061 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.092029095 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.092933893 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.092958927 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.093056917 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.094234943 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.094286919 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.094336987 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.094342947 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.094398022 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.142144918 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.144613028 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.407468081 CET	49716	80	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.412602901 CET	49717	80	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.575942993 CET	80	49716	173.254.29.24	192.168.2.7
Feb 7, 2023 18:30:16.576175928 CET	49716	80	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.582436085 CET	80	49717	173.254.29.24	192.168.2.7
Feb 7, 2023 18:30:16.582645893 CET	49717	80	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.594795942 CET	49717	80	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.762579918 CET	80	49717	173.254.29.24	192.168.2.7
Feb 7, 2023 18:30:16.765436888 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.765480042 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.765707970 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.765759945 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.765769958 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.766005993 CET	443	49711	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.766041994 CET	80	49717	173.254.29.24	192.168.2.7
Feb 7, 2023 18:30:16.766637087 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.766664982 CET	443	49715	142.250.180.174	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:30:16.766843081 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.766853094 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.766875029 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.767014027 CET	443	49714	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.767327070 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.767355919 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.769077063 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.769099951 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.789701939 CET	49718	443	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.789764881 CET	443	49718	173.254.29.24	192.168.2.7
Feb 7, 2023 18:30:16.789889097 CET	49718	443	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.791049957 CET	49718	443	192.168.2.7	173.254.29.24
Feb 7, 2023 18:30:16.791066885 CET	443	49718	173.254.29.24	192.168.2.7
Feb 7, 2023 18:30:16.814109087 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.814193964 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.814217091 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.815141916 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.815251112 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.830034971 CET	49715	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.830066919 CET	443	49715	142.250.180.174	192.168.2.7
Feb 7, 2023 18:30:16.833108902 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.833246946 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.833271980 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.833667994 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.833781958 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.839879990 CET	49712	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.839910984 CET	443	49712	216.58.209.45	192.168.2.7
Feb 7, 2023 18:30:16.842142105 CET	49714	443	192.168.2.7	142.250.180.174
Feb 7, 2023 18:30:16.842158079 CET	49711	443	192.168.2.7	216.58.209.45
Feb 7, 2023 18:30:16.842164993 CET	443	49714	142.250.180.174	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:30:14.183023930 CET	50505	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:14.185152054 CET	61178	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:14.211688042 CET	53	50505	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:14.212719917 CET	53	61178	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:15.309684992 CET	51007	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:15.563178062 CET	53	51007	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:16.990540981 CET	58283	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:17.018524885 CET	53	58283	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:17.841501951 CET	65356	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:17.841568947 CET	59006	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:17.863922119 CET	53	59006	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:18.353802919 CET	51526	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:20.983624935 CET	58746	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:21.003649950 CET	53	58746	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:21.426794052 CET	61248	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:21.446875095 CET	53	61248	8.8.8.8	192.168.2.7
Feb 7, 2023 18:30:42.826637030 CET	53637	53	192.168.2.7	8.8.8.8
Feb 7, 2023 18:30:42.853317976 CET	53	53637	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:30:14.183023930 CET	192.168.2.7	8.8.8.8	0x594	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:14.185152054 CET	192.168.2.7	8.8.8.8	0xeed	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:30:15.309684992 CET	192.168.2.7	8.8.8.8	0xcdc4	Standard query (0)	www.sxconstructions.com.au	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:16.990540981 CET	192.168.2.7	8.8.8.8	0x98d8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:17.841501951 CET	192.168.2.7	8.8.8.8	0x527a	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:17.841568947 CET	192.168.2.7	8.8.8.8	0xd1a2	Standard query (0)	sxcon.b-cdn.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:18.353802919 CET	192.168.2.7	8.8.8.8	0x40a4	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:20.983624935 CET	192.168.2.7	8.8.8.8	0x5852	Standard query (0)	stats.wpmucdn.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:21.426794052 CET	192.168.2.7	8.8.8.8	0xbd5d	Standard query (0)	stats1.wpmudev.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:42.826637030 CET	192.168.2.7	8.8.8.8	0xa21b	Standard query (0)	sxcon.b-cdn.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:30:14.211688042 CET	8.8.8.8	192.168.2.7	0x594	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:14.212719917 CET	8.8.8.8	192.168.2.7	0xeed	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:30:14.212719917 CET	8.8.8.8	192.168.2.7	0xeed	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:15.563178062 CET	8.8.8.8	192.168.2.7	0xcdc4	No error (0)	www.sxconstructions.com.au	sxconstructions.com.au		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:30:15.563178062 CET	8.8.8.8	192.168.2.7	0xcdc4	No error (0)	sxconstructions.com.au		173.254.29.24	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:17.018524885 CET	8.8.8.8	192.168.2.7	0x98d8	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:17.861501932 CET	8.8.8.8	192.168.2.7	0x527a	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:30:17.863922119 CET	8.8.8.8	192.168.2.7	0xd1a2	No error (0)	sxcon.b-cdn.net		89.187.165.194	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:18.375735998 CET	8.8.8.8	192.168.2.7	0x40a4	No error (0)	p.typekit.net	p.typekit.net-stls-v3.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:30:21.003649950 CET	8.8.8.8	192.168.2.7	0x5852	No error (0)	stats.wpmucdn.com	wpmu-stats.b-cdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:30:21.003649950 CET	8.8.8.8	192.168.2.7	0x5852	No error (0)	wpmu-stats.b-cdn.net		89.187.165.194	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:21.446875095 CET	8.8.8.8	192.168.2.7	0xbd5d	No error (0)	stats1.wpmudev.com	matomo-wpmudev-1288779782.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:30:21.446875095 CET	8.8.8.8	192.168.2.7	0xbd5d	No error (0)	matomo-wpmudev-1288779782.us-east-2.elb.amazonaws.com		3.18.180.221	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:30:21.446875095 CET	8.8.8.8	192.168.2.7	0xbd5d	No error (0)	matomo-wpmudev-1288779782.us-east-2.elb.amazonaws.com		3.136.171.197	A (IP address)	IN (0x0001)	false

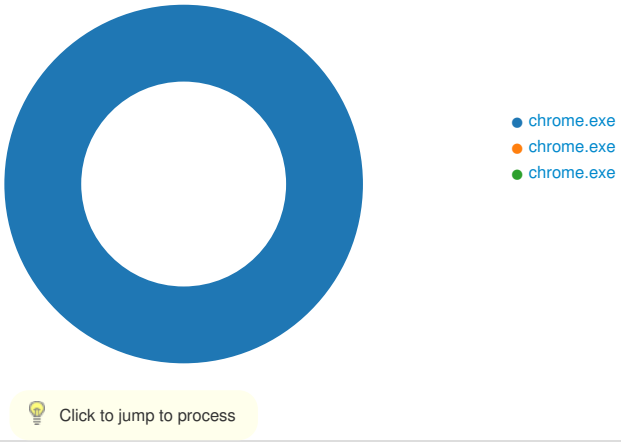
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:30:42.853317976 CET	8.8.8.8	192.168.2.7	0xa21b	No error (0)	sxcon.b-cdn.net		89.187.165.194	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- www.sxconstructions.com.au
- https:
  - sxcon.b-cdn.net
  - stats.wpmucdn.com
  - stats1.wpmudev.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **1768**, Parent PID: **5088**

General

Target ID:	0
Start time:	18:30:09
Start date:	07/02/2023
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:	0x7ff7c2920000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **3480**, Parent PID: **1768**

General

Target ID:	1
Start time:	18:30:10
Start date:	07/02/2023
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=1748 --field-trial-handle=1728,i,14009103719708538658,10673737706731050477,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7c2920000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4368**, Parent PID: **5088**

General

Target ID:	2
Start time:	18:30:11
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.sxconstructions.com.au
Imagebase:	0x7ff7c2920000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly