ID: 876176
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 12:43:28
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

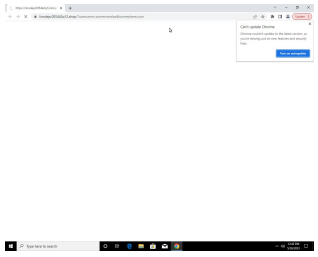
Windows Analysis Report

https://rollins-mkt-prod1.campaign.adobe.com/rln/getImage.jssp?m=ebe0a673-b585-4d5f-8b02-173...

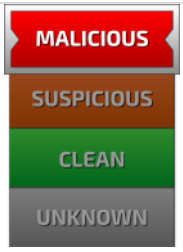
Overview

General Information

Sample URL:	https://rollins-mkt-prod1.campaign.adobe.com/rln/getImage.jssp?m=ebe0a673-b...logo&i=https%3A%2F%2Fstn7ny.codesandbox.io?pop=someone.else%40somewhere.com
Analysis ID:	876176



Detection



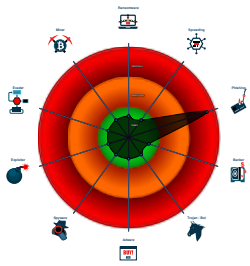
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish54
- Phishing site detected (based on sh…
- Phishing site detected (based on im…
- HTML page contains hidden URLs o…
- Yara signature match
- Detected hidden input values contai…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 3004 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://rollins-mkt-prod1.campaign.adobe.com/rln/getImage.jssp?m=ebe0a673-b585-4d5f-8b02-173d6da0ca15&e=boss&l=brandlogo&i=https%3A%2F%2Fstn7ny.codesandbox.io?pop=someone.else%40somewhere.com MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 4180 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=2044 --field-trial-handle=1780,i,4533431973836403822,16059512273480551448,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
2.2.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x5b34:$c8: while(!![]) • 0x5b52:$d1: parseInt(_0xc5ee45(0x26f))/0x1+-parseInt(_0xc5ee45(0x234))/0x2*(-parseInt(_0xc5ee45(0x282))/0x3)+parseInt(_0xc5ee45(0x292))/0x4+-parseInt(_0xc5ee45(0x18b))/0x5+parseInt(_0xc5ee45(0x269))/0x6+- • 0x5b72:$d1: parseInt(_0xc5ee45(0x234))/0x2*(-parseInt(_0xc5ee45(0x282))/0x3)+parseInt(_0xc5ee45(0x292))/0x4+- parseInt(_0xc5ee45(0x18b))/0x5+parseInt(_0xc5ee45(0x269))/0x6+-parseInt(_0xc5ee45(0x149))/0x7*(• 0x5b93:$d1: parseInt(_0xc5ee45(0x282))/0x3)+parseInt(_0xc5ee45(0x292))/0x4+-parseInt(_0xc5ee45(0x18b))/0x5+parseInt(_0xc5ee45(0x269))/0x6+-parseInt(_0xc5ee45(0x149))/0x7*(parseInt(_0xc5ee45(0x563))/0x8)+- • 0x55d84:$d1: parseInt(_0x19263b(0x158))/0x1+-parseInt(_0x19263b(0x10f))/0x2+-parseInt(_0x19263b(0x15e))/0x3+-parseInt(_0x19263b(0x150))/0x4*(-parseInt(_0x19263b(0xfe))/0x5)+parseInt(_0x19263b(0x13c))/0x6*(• 0x55da4:$d1: parseInt(_0x19263b(0x10f))/0x2+-parseInt(_0x19263b(0x15e))/0x3+-parseInt(_0x19263b(0x150))/0x4*(-parseInt(_0x19263b(0xfe))/0x5)+parseInt(_0x19263b(0x13c))/0x6*(parseInt(_0x19263b(0x159))/0x7)+- • 0x55dc4:$d1: parseInt(_0x19263b(0x15e))/0x3+-parseInt(_0x19263b(0x150))/0x4*(- parseInt(_0x19263b(0xfe))/0x5)+parseInt(_0x19263b(0x13c))/0x6*(parseInt(_0x19263b(0x159))/0x7)+-parseInt(_0x19263b(0x10d))/0x8+
2.3.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x264bc:$c8: while(!![]) • 0x264db:$d1: parseInt(_0x2c029d(0x134))/0x1*(parseInt(_0x2c029d(0x3aa))/0x2)+- parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+- • 0x264fb:$d1: parseInt(_0x2c029d(0x3aa))/0x2)+-parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+- • 0x2651c:$d1: parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(• 0x2653c:$d1: parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(parseInt(_0x2c029d(0x2d2))/0x9)+- • 0x2655c:$d1: parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+- parseInt(_0x2c029d(0x1a3))/0x7+- parseInt(_0x2c029d(0x144))/0x8*(parseInt(_0x2c029d(0x2d2))/0x9)+-parseInt(_0x2c029d(0x256))/0xa*(- • 0x68e66:$d1: parseInt(_0x44edb5(0x197))/0x1+parseInt(_0x44edb5(0x191))/0x2+-parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(• 0x68e85:$d1: parseInt(_0x44edb5(0x191))/0x2+-parseInt(_0x44edb5(0x1b9))/0x3+- parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+ • 0x68ea5:$d1: parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6* (parseInt(_0x44edb5(0x1cb))/0x7)+parseInt(_0x44edb5(0x1c7))/0x8*(- • 0x68ec5:$d1: parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6* (parseInt(_0x44edb5(0x1cb))/0x7)+parseInt(_0x44edb5(0x1c7))/0x8*(-parseInt(_0x44edb5(0x1c3))/0x9)+
2.3.pages.csv	JoeSecurity_HtmlPhish_54	Yara detected HtmlPhish_54	Joe Security	

Source	Rule	Description	Author	Strings
3.5.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x6ed1:$c8: while(!![]) • 0x6ef0:$d1: parseInt(_0x2c029d(0x134))/0x1*(parseInt(_0x2c029d(0x3aa))/0x2)+-parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+- • 0x6f10:$d1: parseInt(_0x2c029d(0x3aa))/0x2)+-parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+- • 0x6f31:$d1: parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(• 0x6f51:$d1: parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(parseInt(_0x2c029d(0x2d2))/0x9)+- • 0x6f71:$d1: parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(parseInt(_0x2c029d(0x2d2))/0x9)+-parseInt(_0x2c029d(0x256))/0xa*(- • 0x49873:$d1: parseInt(_0x44edb5(0x197))/0x1+parseInt(_0x44edb5(0x191))/0x2+-parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(• 0x49892:$d1: parseInt(_0x44edb5(0x191))/0x2+-parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+ • 0x498b2:$d1: parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+parseInt(_0x44edb5(0x1c7))/0x8*(- • 0x498d2:$d1: parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+parseInt(_0x44edb5(0x1c7))/0x8*(-parseInt(_0x44edb5(0x1c3))/0x9)+

Source	Rule	Description	Author	Strings
3.4.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x6ed1:$c8: while(!![]) • 0x6ef0:$d1: parseInt(_0x2c029d(0x134))/0x1*(parseInt(_0x2c029d(0x3aa))/0x2)+-parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+- • 0x6f10:$d1: parseInt(_0x2c029d(0x3aa))/0x2)+-parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+- • 0x6f31:$d1: parseInt(_0x2c029d(0x448))/0x3*(parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(• 0x6f51:$d1: parseInt(_0x2c029d(0x1f4))/0x4)+parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(parseInt(_0x2c029d(0x2d2))/0x9)+- • 0x6f71:$d1: parseInt(_0x2c029d(0x44a))/0x5+parseInt(_0x2c029d(0x2f6))/0x6+-parseInt(_0x2c029d(0x1a3))/0x7+-parseInt(_0x2c029d(0x144))/0x8*(parseInt(_0x2c029d(0x2d2))/0x9)+-parseInt(_0x2c029d(0x256))/0xa*(- • 0x49873:$d1: parseInt(_0x44edb5(0x197))/0x1+parseInt(_0x44edb5(0x191))/0x2+-parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(• 0x49892:$d1: parseInt(_0x44edb5(0x191))/0x2+-parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+ • 0x498b2:$d1: parseInt(_0x44edb5(0x1b9))/0x3+-parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+parseInt(_0x44edb5(0x1c7))/0x8*(- • 0x498d2:$d1: parseInt(_0x44edb5(0x1c0))/0x4*(parseInt(_0x44edb5(0x1bc))/0x5)+parseInt(_0x44edb5(0x1d3))/0x6*(parseInt(_0x44edb5(0x1cb))/0x7)+parseInt(_0x44edb5(0x1c7))/0x8*(-parseInt(_0x44edb5(0x1c3))/0x9)+
Click to see the 2 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Phishing site detected (based on favicon image match)
Yara detected HtmlPhish54
Phishing site detected (based on shot match)
Phishing site detected (based on image similarity)

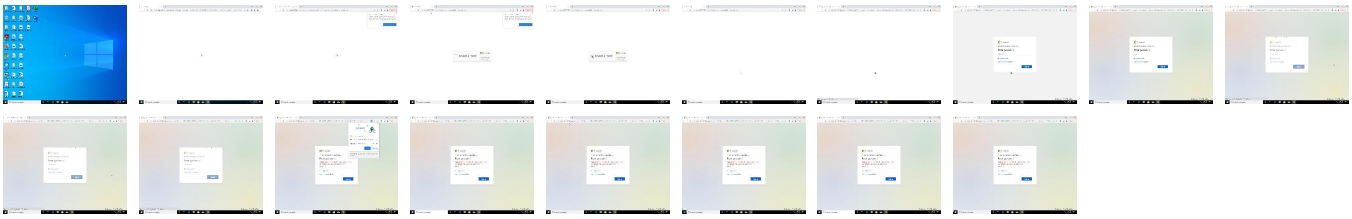
Mitre Att&ck Matrix

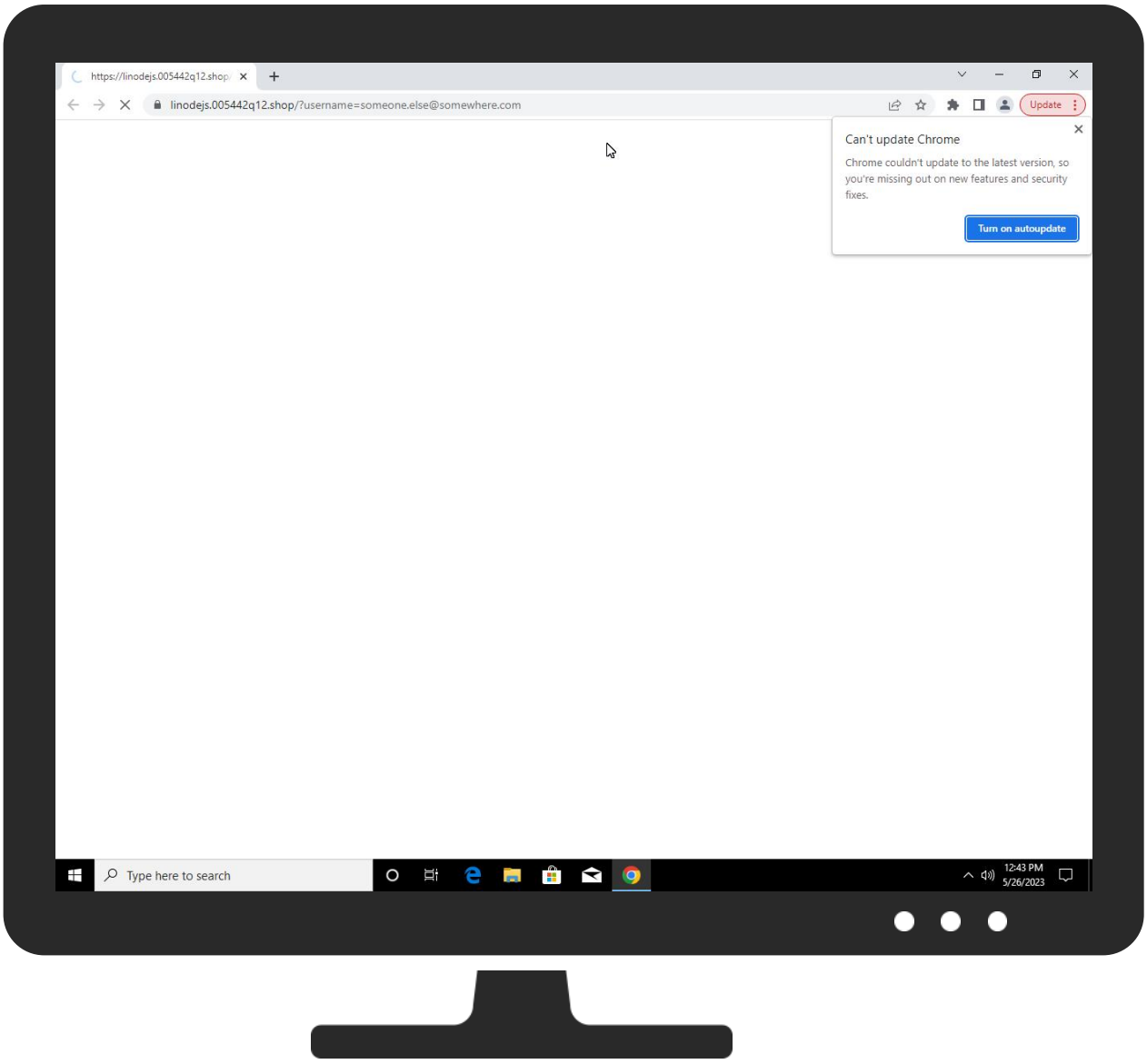
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 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	1 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	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
https://rollins-mkt-prod1.campaign.adobe.com/rln/getImage.jssp?m=ebe0a673-b585-4d5f-8b02-173d6da0ca15&e=boss&l=brandlogo&i=https%3A%2F%2Fstn7ny.codesandbox.io?pop=someone.else%40somewhere.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

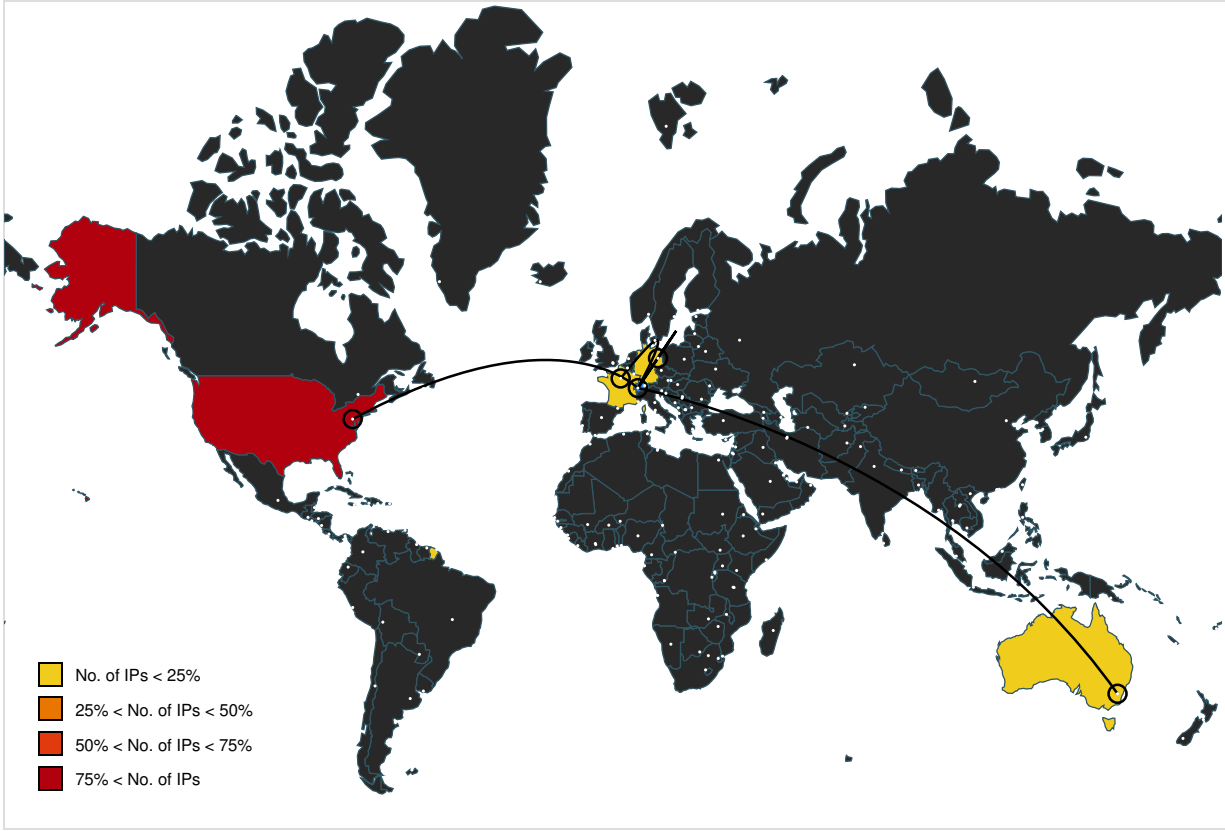
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stn7ny.codesandbox.io	104.18.6.114	true	false		high
2dc78927-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
static.cloudflareinsights.com	104.16.57.101	true	false		unknown
data-jsdelivr-com.b-cdn.net	138.199.37.231	true	false		high
5ea3126c-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
accounts.google.com	216.58.212.173	true	false		high
codesandbox.io	104.18.6.114	true	false		high
4f1681c3-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
prod-packager-packages.codesandbox.io	104.18.6.114	true	false		high
60a80c15-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
a74daa9e-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
c75aac07-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
col.csbops.io	148.251.96.176	true	false		unknown
a14e93ae-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
313cb46a-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
e5c1f986-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
thehareatoldredding.com	54.36.33.112	true	false		unknown
linodejs.005442q12.shop	94.247.42.35	true	false		unknown
www.google.com	172.217.16.196	true	false		high
5a236ad3-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
account.005442q12.shop	94.247.42.35	true	false		unknown
clients.l.google.com	142.250.185.174	true	false		high
live.005442q12.shop	94.247.42.35	true	false		unknown
56da54a3-ba9ad70d.005442q12.shop	94.247.42.35	true	false		unknown
clients2.google.com	unknown	unknown	false		high
data.jsdelivr.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
about:blank	false		low
https://thehareatoldredding.com/quickactions/werking/lobatan/jhfhejrejre/someone.else@somewhere.com	false		unknown
https://live.005442q12.shop/ppsecure/post.srf?client_id=51483342-085c-4d86-bf88-cf50c7252078&contextid=00B77BF5E430D8A6&opid=0B96B26FFA9F979B&bk=1685097846&uaid=101285ee581b4befaf82bf9d60446afd&pid=15216	false		unknown
https://linodejs.005442q12.shop/?username=someone.else@somewhere.com	true		unknown
https://live.005442q12.shop/oauth20_authorize.srf?scope=openid+profile+email+offline_access&response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&response_mode=form_post&redirect_uri=https%3a%2f%2flinodejs.005442q12.shop%2fcommon%2ffederation%2foauth2msa&state=rQQIARAA42Kw0skoKSkottLXL8gvKknM0cvNTC7KL85PK8nPy8nMS9VLzs_Vyy9Kz0wBsYqEuATetQoJSEe8917ftH9ugkvW31mMnPE5mWVglasYlQkbp3-BkfEFI-MkJqni_NzUfKBgak5xqgOIU56RWgRWc4tJ0L8o3TMlvNgtNSW1KLEkMz_vETMeDRdYBF6x8BgwW3FwcAkwSDAoMPxgYVzECnSv1iWziKWt-T4zs6N6GYw1GE6x6mcHFwZpp7uVmZh6RJU555ZWJVflVSQWJAV5pZpGGjm5WSR5haU4phnpVybbmlsZTmATmsDGdlqN4QMbYwc7wyx2hgOcjBt4GA_wMvzgu79ka_OjXdfferzi16ksjPBxLEqNDHKvqnKrCCvOSw_IDC3MCzU1NMkxLUtxLTe3zHSNdAytdPK1BQA1&login_hint=someone.else%40somewhere.com&estsfed=1&uaid=101285ee581b4befaf82bf9d60446afd&fci=https%3a%2f%2fportal.microsoftonline.com.orgid.com#	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.68	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
138.199.37.231	data-jsdelivr-com.b-cdn.net	European Union		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
148.251.96.176	col.csbops.io	Germany		24940	HETZNER-ASDE	false
142.250.185.227	unknown	United States		15169	GOOGLEUS	false
142.250.181.227	unknown	United States		15169	GOOGLEUS	false
104.18.6.114	stn7ny.codesandbox.io	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.174	clients.l.google.com	United States		15169	GOOGLEUS	false
104.16.57.101	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false
54.36.33.112	thehareatoldredding.com	France		16276	OVHFR	false
216.58.212.173	accounts.google.com	United States		15169	GOOGLEUS	false
34.215.187.240	unknown	United States		16509	AMAZON-02US	false
172.217.18.10	unknown	United States		15169	GOOGLEUS	false
172.217.16.196	www.google.com	United States		15169	GOOGLEUS	false
94.247.42.35	2dc78927-ba9ad70d.005442q12.shop	Germany		34549	MEER-ASmeerfarbigGmbHCoKGDE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876176
Start date and time:	2023-05-26 12:43:28 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://rollins-mkt-prod1.campaign.adobe.com/rln/getImage.jssp?m=ebe0a673-b585-4d5f-8b02-173d6da0ca15&e=boss&l=brandlogo&i=https%3A%2F%2Fstn7ny.codesandbox.io?pop=someone.else%40somewhere.com
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	4
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@27/126@35/160

Warnings

- Exclude process from analysis (whitelisted): svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.181.227, 34.215.187.240, 34.104.35.123, 172.217.18.10, 172.217.16.138, 142.250.186.106, 142.250.186.74, 172.217.16.202, 142.250.185.234, 142.250.185.138, 142.250.185.106, 142.250.185.74, 172.217.18.106, 172.217.23.106, 142.250.181.234, 216.58.212.170, 216.58.212.138, 142.250.185.202, 142.250.185.170
- Excluded domains from analysis (whitelisted): rollins-mkt-prod1.campaign.adobe.com, rollins-mkt-prod1-1.campaign.adobe.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: https://linodejs.005442q12.shop/?username=someone.else@somewhere.com

Created / dropped Files

Chrome Cache Entry: 174

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):	71919
Entropy (8bit):	5.303739091278291
Encrypted:	false
SSDEEP:	
MD5:	12BBC52470D80AD262344088C3258EC8
SHA1:	17FE61AE5ACF2A216F0F7536FE3C5151E4917384
SHA-256:	2FCC1563896A5072C48A977C92617765CD7458FA5845D9F119D9BFF185B54BCE
SHA-512:	1B6475DFB317F112EB808C87E773D88159EF25174CE2FB1BBF96969B955D09C5A5E5E6E8118BB72D142CCDA7365CAC049D7C2C18642BB6A1DE45E3530CD6905
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/default~app~embed~sandbox.5ecd4ceea.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["default~app~embed~sandbox"],{"../../standalone-packages/codesandbox-browserfs/dist/shims/fs.js":function(e,t){e.exports=BrowserFS.BFSRequire("fs")},"../common/lib/forked-vendors/jsonlint.browser.js":function(e,t,s){"use strict";var o,n,i=(o={trace:function(){},yy:{},symbols_:{error:2,JSONString:3,STRING:4,JSONNumber:5,NUMBER:6,JSONNullLiteral:7,NULL:8,JSONBooleanLiteral:9,TRUE:10,FALSE:11,JSONText:12,JSONValue:13,EOF:14,JSONObject:15,JSONArray:16,"{":17,"}":18,JSONMemberList:19,JSONMember:20,":":21,",":22,"[":23,"]":24,JSONElementList:25,$accept:0,$end:1},terminals_:{2:"error",4:"STRING",6:"NUMBER",8:"NULL",10:"TRUE",11:"FALSE",14:"EOF",17:"{",18:"}",21:":",22:",",23:"[",24:"]"},productions_:[0,[3,1],[5,1],[7,1],[9,1],[9,1],[12,2],[13,1],[13,1],[13,1],[13,1],[13,1],[13,1],[15,2],[15,3],[20,3],[19,1],[19,3],[16,2],[16,3],[25,1],[25,3]],performAction:function(e,t,s,o,n,i,r){var a=i.length-1;switch(n){case 1:this.$=e.replace(/\\(\\\|")/g,"$1").repl

Chrome Cache Entry: 175

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	1877
Entropy (8bit):	3.88650701777189

Encrypted:	false
SSDEEP:	
MD5:	9E04FEF372286303412D74EA27F8C768
SHA1:	05BA0A93781984A71758629DFD68BE9772C247CB
SHA-256:	C2DF9C4E9E2A6343566A5F6D067D3BC187717A5E9A01F6BF6808AF6314F52CCF
SHA-512:	1F72266EFD2789F8EA8CFFCA3ECE101FD1014681FB452ED9229EDBDCDB3B80EE9CA6DF7E96F29A43D97849A273825FD222DD660DD0DA7333BE36F78298563E90
Malicious:	false
Reputation:	low
URL:	https://data.jsdelivr.com/v1/package/npm/@babel/runtime
Preview:	{.."tags": {..."latest": "7.21.5",..."broken": "7.12.17",..."esm": "7.21.4-esm.4"..},.."versions": [..."7.21.5",..."7.21.4-esm.4",..."7.21.4-esm.3",..."7.21.4-esm.2",..."7.21.4-esm.1",..."7.21.4-esm",..."7.21.0",..."7.20.13",..."7.20.7",..."7.20.6",..."7.20.5",..."7.20.1",..."7.20.0",..."7.19.4",..."7.19.0",..."7.18.9",..."7.18.6",..."7.18.3",..."7.18.2",..."7.18.0",...."7.17.9",..."7.17.8",..."7.17.7",..."7.17.2",..."7.17.0",..."7.16.7",..."7.16.5",..."7.16.3",..."7.16.0",..."7.15.4",..."7.15.3",..."7.14.8",..."7.14.6",..."7.14.5",..."7.14.0",..."7.13.17",..."7.13.16",..."7.13.10",..."7.13.9",..."7.13.8",..."7.13.7",..."7.13.6",..."7.13.4",..."7.13.2",..."7.13.1",..."7.13.0",..."7.12.18",..."7.12.17",..."7.12.13",..."7.12.5",..."7.12.1",..."7.12.0",..."7.11.2",..."7.11.1",..."7.11.0",..."7.10.5",..."7.10.4",..."7.10.3",..."7.10.2",..."7.10.1",..."7.10.0",..."7.9.6",..."7.9.2",..."7.9.0",..."7.8.7",..."7.8.4",..."7.8.3",..."7.8.0",..."7.7.7",..."7.7.6",..."7.7.5",..."7.7.4",..."7.7.2",.

Chrome Cache Entry: 176

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (16846)
Category:	downloaded
Size (bytes):	16924
Entropy (8bit):	5.171111765536655
Encrypted:	false
SSDEEP:	
MD5:	1D4092572D730BD2AF5618481FF8D9CE
SHA1:	B98A5A579E1E9973098587C6A431AF158E2A75FA
SHA-256:	49882B4768F3155504BF1919726C430D358DEEAB783A6B5DB9197B9999193CE8
SHA-512:	204890C631EDF348D7410F47899FBA2D96B66DE6294245AE5F5DAD60CB0FD56A67D61BFAE0406054779973124 49B950C6BEBE5CA4CACFA277DCAC411B7718EDD
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/vendors~app~embed~sandbox-startup.b754f8b0e.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["vendors~app~embed~sandbox-startup"],{"../../node_modules/console-feed/lib/Hook/index.js":function(e,t,r){"use strict";t.__esModule=!0;var n=r("../../node_modules/console-feed/lib/definitions/Methods.js"),o=r("../../node_modules/console-feed/lib/Hook/parse/index.js"),a=r("../../node_modules/console-feed/lib/Transform/index.js");t.default=function(e,t,r){void 0===r&&(r=!0);for(var i=e,s={pointers:{},src:{npm:"https://npmjs.com/package/console-feed",github:"https://github.com/samdenty99/console-feed"}},u=function(e){var n=i[e];i[e]=function(){n.apply(this,arguments);var i=[].slice.call(arguments);setTimeout((function(){var n=o.default(e,i);if(n){var s=n;r&&(s=a.Encode(n)),t(s,n)}}))},s.pointers[e]=n},f=0,l=n.default;f<l.length;f++)u(l[f]);return i.feed=s,i}},"../../node_modules/console-feed/lib/Hook/parse/GUID.js":function(e,t,r){"use strict";t.__esModule=!0,t.default=function(){var e=function(){return(65536*(1+Math.random())|0).toString(16).subs

Chrome Cache Entry: 177

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (3850)
Category:	downloaded
Size (bytes):	3895
Entropy (8bit):	5.169182983164913
Encrypted:	false
SSDEEP:	
MD5:	D071B69DD295C87D7145C6296CB6DE04
SHA1:	A01E4EFB6F459F2C9751C45AA98E483FBE920031
SHA-256:	683FBDEF88B2EBF85E44C498687952697F4093FB1FF40F884EB6A2F3C74D0BB7
SHA-512:	B6DB3ED024AB5C111C4D3F1DA2756F49948585F30383682B7B85D8CC83F82BE5B370C89630F1ACF284B95C32986D44DCDB8A6509440E195D22A9FEB9CC13DEA
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/banner.0b5d84a2b.js
Preview:	!function(n){var e={};function t(o){if(e[o])return e[o].exports;var r=e[o]={i:o,l:!1,exports:{}};return n[o].call(r.exports,r,r.exports,t),r.l=!0,r.exports}t.m=n,t.c=e,t.d=function(n,e,o){t.o(n,e)||Object.defineProperty(n,e,{enumerable:!0,get:o})},t.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,e){if(1&e&&(n=t(n)),8&e)return n;if(4&e&&"object"==typeof n&&n&&n.__esModule)return n;var o=Object.create(null);if(t.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:n}),2&e&&"string"!=typeof n)for(var r in n)t.d(o,r,function(e){return n[e]}.bind(null,r));return o},t.n=function(n){var e=n&&n.__esModule?function(){return n.default}:function(){return n};return t.d(e,"a",e),e},t.o=function(n,e){return Object.prototype.hasOwnProperty.call(n,e)},t.p="https://codesandbox.io/",t(t.s="./src/banner.js")}({"./src/banner.js":function(n,e){var t;var o=funct

Chrome Cache Entry: 178

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, 16x16 with PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced, 32 bits/pixel, 24x24 with PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced, 32 bits/pixel
Category:	downloaded
Size (bytes):	2279
Entropy (8bit):	7.354295352983905
Encrypted:	false
SSDEEP:	
MD5:	7E0D59593F3377B72C29435C4B43954A
SHA1:	B4C5C39A6DFB460BBD2EACCEB09EC8079FB6A8E2
SHA-256:	62D706019A0D80173113EF70FBBEE12F286E8E221534BE788448AADA4B14C8E8
SHA-512:	397416A6A96A39F46F22E906A60E56067E5B7B11FB0597A733F862FC077C88D5ED31F51A82709A56F6082FB1F2F72F9A0FE0849E3DD493BB4240C265B546AAD3
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/16.000.29808.2/images/favicon.ico
Preview:	....f..... .$...|... .... .5.....00.... .j.....@@.... .....?..... .....2....PNG.....IHDR.....a....IDATx..1NCA.C..D@."-en.!.h..8@..9h.."....5M....h..-..l..L..P.Y.^luw...r.(.....w...B({....&.F.....N.f%.....^&.x}Zu.....g..7m.....n?..U`....@.M8.g.-..|..S.K.!....].%.l.....&.l..`...F \|o;....{S....\|..VL...E*....IEND.B`..PNG.....IHDR.....w=.....IDATx..AJ.A.E_.5...D..$'....<.g.\....!.].!..Y....4...B.....4U...Q..J(...y....%..[t;..>\...~....O....r.....e...F....8.d9....4.x.x*W..e...c...~W..P2.....[.....r<...,..>....q.\...U...v.'.....!.1....9..:8.....l.l.d.....IEND.B`..PNG.....IHDR... ... .szz.....IDATx..AJC1.E.{..... .;..>\..q+.. ..N.j....."8k.P..IF...M..{.8..F..Z.q...~.y}...0.f..U....Z...@yd...4.....DT.B..).....v.8.....)..Lq.[. ...]_jrG$...3.%.....i.vU...C...h0.....rz^.].....9..5.....mU~.E..GMF.X....?..Y.U..|.c.k.v>..@.h.....Nh.u.....IEND.B`..PNG.....IHDR...

Chrome Cache Entry: 179

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 152 x 152, 8-bit grayscale, non-interlaced
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.398173229936654
Encrypted:	false
SSDEEP:	
MD5:	1A451AE3B6D39377159936F9E62D1E91
SHA1:	9F3B7EA363B357064A2FF92283FECF5210396611
SHA-256:	DF5287DDBFA0B397B85636AEBB1C0DA128E595D5F1ED3EDBA3465B5C73D48DFE
SHA-512:	64A2C02C3A60EFD06B054C39C5A32B7AEC69AA6E99E2187297D1C837F85D94343744A6791ACC13648FA2A0DF20F1A4D79C015BCF8581EBAE3D1878CF6CFD6EFA
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....=.....gAMA.....a.....sRGB.....IDATx...A.. .@AJh.0R...@L...;?..~.>Z.....{.....,..b"..,.....K.....``+.v.&.F....o.....%..|o..`.v....IEND.B`.

Chrome Cache Entry: 181

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 182

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	83140
Entropy (8bit):	4.978749099677931
Encrypted:	false
SSDEEP:	
MD5:	3A1DEFB24008E857FE947FDF438749C7
SHA1:	D4269EB45F87C634FE7F97D67EA30239D1D9F6EE
SHA-256:	873F553C14A1E67D4079F3ACFD754B180E9DDDD677FC20D0CCE6C1D84DF128FC
SHA-512:	CC16E37BFC30C77E2A007139AE34245480B749B3BBEAC4E71A7E7AA4AF3E738E557CA2D03EC3817144759807B3649A43B0C96C56B1C386B7615922BBEA9402C2
Malicious:	false
Reputation:	low
URL:	https://prod-packager-packages.codesandbox.io/v2/packages/node-libs-browser/2.2.1.json
Preview:	{"contents":{"/node_modules/asn1.js/package.json":{"content":"{\"name\":\"asn1.js\",\"version\":\"5.4.1\",\"description\":\"ASN.1 encoder and decoder\",\"main\":\"lib/asn1.js\",\"scripts\":{\"lint-2560\":\"eslint --fix rfc/2560/*.js rfc/2560/test/*.js\",\"lint-5280\":\"eslint --fix rfc/5280/*.js rfc/5280/test/*.js\",\"lint\":\"eslint --fix lib/*.js lib/**/*.js lib/**/**/*.js && npm run lint-2560 && npm run lint-5280\",\"test\":\"mocha --reporter spec test/*-test.js && cd rfc/2560 && npm i && npm test && cd ../../rfc/5280 && npm i && npm test && cd ../../ && npm run lint\"},\"repository\":{\"type\":\"git\",\"url\":\"git@github.com:indutny/asn1.js\"},\"keywords\":[\"asn.1\",\"der\"],\"author\":\"Fedor Indutny\",\"license\":\"MIT\",\"bugs\":{\"url\":\"https://github.com/indutny/asn1.js/issues\"},\"homepage\":\"https://github.com/indutny/asn1.js\",\"devDependencies\":{\"eslint\":\"^4.10.0\",\"mocha\":\"^7.0.0\"},\"dependencies\":{\"bn.js\":\"^4.0.0\",\"inherits\":\"^2.0.1\",\"minimalistic-

Chrome Cache Entry: 183

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2734)
Category:	downloaded
Size (bytes):	2789
Entropy (8bit):	5.228455537563853
Encrypted:	false
SSDEEP:	
MD5:	8D1B32D2C888E49391B924D7EE395C1F
SHA1:	C4EA654D576151A063040734935CFD7CF2A7FA77
SHA-256:	F74BF2CF5A8225BEB66712FF4E859C5D4BA9C24123E6DE2F427B4B9FDE408928
SHA-512:	E6FAF9E2DD7EA5730415285FD82271CCB62792EB2A7BFAC6C4647A61EA2988B2AA28B7F75ED8E0C4E262116DE9379DFF32E2E84DC123D97DED3BC64CDD6F53FF
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/watermark-button.f4f9aed52.js
Preview:	!function(n){var e={};function t(o){if(e[o])return e[o].exports;var r=e[o]={i:o,l:!1,exports:{}};return n[o].call(r.exports,r,r.exports,t),r.l=!0,r.exports}t.m=n,t.c=e,t.d=function(n,e,o){t.o(n,e)||Object.defineProperty(n,e,{enumerable:!0,get:o})},t.r=function(n){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,e){if(1&e&&(n=t(n)),8&e)return n;if(4&e&&"object"==typeof n&&n&&n.__esModule)return n;var o=Object.create(null);if(t.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:n}),2&e&&"string"!=typeof n)for(var r in n)t.d(o,r,function(e){return n[e]}.bind(null,r));return o},t.n=function(n){var e=n&&n.__esModule?function(){return n.default}:function(){return n};return t.d(e,"a",e),e},t.o=function(n,e){return Object.prototype.hasOwnProperty.call(n,e)},t.p="https://codesandbox.io/",t(t.s="./src/watermark-button.js")}({"./src/watermark-button.js":function(n,

Chrome Cache Entry: 184

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (64605)
Category:	downloaded
Size (bytes):	411897
Entropy (8bit):	5.454154047429814
Encrypted:	false
SSDEEP:	
MD5:	E9C34E4F7E8595486559B9E553FEC63B
SHA1:	734743FC1DAC7AFD79B86D3B7058E50954F24F5D
SHA-256:	22540965A6508A6125BAF4468E02E81EABE7C1699E623A1C9351118BB60F8CFD
SHA-512:	FCD009B899D60449E8471B0BF33DB056347F6FFAD312F0FFF6DC65B9FF9619740B0A73AC3919ED2F72F1E7295715E7F5AAFE9E0BEA6BCE411203F71BD1D5561C
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/js/ConvergedLogin_PCore_OpV8E9t-Hkyo-3QO1GFC6Q2.js

Preview:	/*! * ---------- START OF THIRD PARTY NOTICE ----------. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.005442q12 .shop/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * ---------- END OF THIRD PARTY NOTICE ----------. */!function(e){function n(n){for(var t,i,o=n[0],r=n[1],s=0,c=[];s<o.

Chrome Cache Entry: 185	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (10357)
Category:	downloaded
Size (bytes):	10411
Entropy (8bit):	5.250209634077698
Encrypted:	false
SSDEEP:	
MD5:	C6D47800AC85C92F177F69B933B3C8E2
SHA1:	1FD00FDB29B97760A4F139D02FF8261B1B15B0D5
SHA-256:	E05B0AF05F3BB9E5D06C3AB2C2ADF581131CD51AFA004F39F303A1D2F3EB321D
SHA-512:	F59DB37FE2708312C7D34113123A7EB419D052C4ED67FD6975241F136092669F3F4E55D6EC691D27A21E620DE4C817AC0B56F0169AA3109499853230F022D3AB
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/sandbox-startup.a6840230d.js
Preview:	!function(e){function t(t){for(var o,a,i=t[0],c=t[1],d=t[2],l=0,f=[];l<i.length;l++)a=i[l],Object.prototype.hasOwnProperty.call(r,a)&&r[a]&&f.push(r[a][0]),r[a]=0;for(o in c)Object .prototype.hasOwnProperty.call(c,o)&&(e[o]=c[o]);for(u&&u(t);f.length;)f.shift()();return s.push.apply(s,d||[]),n()}function n(){for(var e,t=0;t<s.length;t++){for(var n=s[t],o=!0,i =1;i<n.length;i++){var c=n[i];0!==r[c]&&(o=!1)}o&&(s.splice(t--,1),e=a(a.s=n[0]))}return e}var o={},r={"sandbox-startup":0},s=[];function a(t){if(o[t])return o[t].exports;var n=o[t]={i:t,l:!1,exports:{}};return e[t].call(n.exports,n,n.exports,a),n.l=!0,n.exports}a.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.push(n[2]);else{var o=new Promise((function(t,o){ n=r[e]=[t,o]}));t.push(n[2]=o);var s,i=document.createElement("script");i.charset="utf-8",i.timeout=120,a.nc&&i.setAttribute("nonce",a.nc),i.src=function(e){return a.p+"s tatic/js/"+({}[e]||e)+"."+{4:"0b6613143",5:"4c4f58c53"}[e]+".chunk.js"}(e);var c=new Error;s=function(t){i.one

Chrome Cache Entry: 186	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (19108), with no line terminators
Category:	downloaded
Size (bytes):	19108
Entropy (8bit):	5.2019686611389435
Encrypted:	false
SSDEEP:	
MD5:	032525749D7C7529984CB68D00A13DF1
SHA1:	D11A04017315D4022473FD91877CDD3D52409F18
SHA-256:	707F25811CF0BF4235F64F3D620A3D6D2040CE85EBB5CFF815B4148472B77219
SHA-512:	64B952AA5532F9316A352BF16D7E9C2F9D21D137459613803D4D7037785BCEA9B4591E62DD31578ABD1EA5BDE3A29F777BC0BD9F6036D5F0484CAA655A2F97E 5
Malicious:	false
Reputation:	low
URL:	https://stn7ny.codesandbox.io/sandbox-service-worker.js
Preview:	"use strict";var precacheConfig=[["frame.html","49a5e7603d7fec7e59c436ae704a9399"]],cacheName="sw-precache-v3-code-sandbox-sandbox-"+(self.registration? self.registration.scope:""),ignoreUrlParametersMatching=[/^utm_/],addDirectoryIndex=function(e,t){var n=new URL(e);return"/"===n.pathname.slice(-1)&&(n.pathna me+=t),n.toString()},cleanResponse=function(e){return e.redirected?("body"in e?Promise.resolve(e.body):e.blob()).then(function(t){return new Response(t,{headers :e.headers,status:e.status,statusText:e.statusText})}):Promise.resolve(e)},createCacheKey=function(e,t,n,r){var o=new URL(e);return r&&o.pathname.match(r)||(o.s earch+=(o.search?"&":"")+encodeURIComponent(t)+"="+encodeURIComponent(n)),o.toString()},isPathWhitelisted=function(e,t){if(0===e.length)return!0;var n=new URL(t).pathname;return e.some(function(e){return n.match(e)})},stripIgnoredUrlParameters=function(e,t){var n=new URL(e);return n.hash="",n.search=n.search.slice(1).s plit("&").map(function(e){return e.split("=")}).fi

Chrome Cache Entry: 187	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	426119
Entropy (8bit):	5.605066401860902
Encrypted:	false
SSDEEP:	
MD5:	17643BBF7A4F50525555F34A5FCDEB82
SHA1:	2B6ECBEC1296F70A4F8CABB39E1B0C439FCB36DA
SHA-256:	7D16A81451DC4157397D6D615F7A38D5986DF5D2667AAE6A934B77B9F4E792B9

SHA-512:	5B9E7015EDBDA16B95331556DC9EED2BD56B86EBC0FFC18DC621F26A174322812C1C224A12F49A8A7147137E23B44D32BF8BF68149693DF25FA40C8E5729E10 0
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/vendors~sandbox.3bd3135bd.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["vendors~sandbox"],{"../../node_modules/@babel/runtime/helpers/toArray.js":function(e,t,n){var r=n("../../node_modules/ @babel/runtime/helpers/arrayWithHoles.js"),o=n("../../node_modules/@babel/runtime/helpers/iterableToArray.js"),u=n("../../node_modules/@babel/runtime/helpers/un supportedIterableToArray.js"),i=n("../../node_modules/@babel/runtime/helpers/nonIterableRest.js");e.exports=function(e){return r(e)||o(e)||u(e)||i()}},"../../node_modules /anser/lib/index.js":function(e,t,n){"use strict";var r=u(n("../../node_modules/babel-runtime/helpers/classCallCheck.js")),o=u(n("../../node_modules/babel-runtime/helpers /createClass.js"));function u(e){return e&&e.__esModule?e:{default:e}}var i=[[{color:"0, 0, 0",class:"ansi-black"},{color:"187, 0, 0",class:"ansi-red"},{color:"0, 187, 0" ,class:"ansi-green"},{color:"187, 187, 0",class:"ansi-yellow"},{color:"0, 0, 187",class:"ansi-blue"},{color:"187, 0, 187",class:"ansi-magenta"},{color:"0, 187, 187",class

Chrome Cache Entry: 189

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-col or="#c4c4c4" stop-opacity="0"/></radialGradient><r

Chrome Cache Entry: 190

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	1223
Entropy (8bit):	4.472668858062847
Encrypted:	false
SSDEEP:	
MD5:	FE74E9F39ACDF2B10B95B97E4F118786
SHA1:	F61FC4F7157785C964E23A8A5045B2A34FDAFFB1
SHA-256:	52111D502CF34DA8573D4A271391DA77E0B79170F82D5638A4E67D5F328B9320
SHA-512:	AE6CA63F11EC52F9A60F9908505184AD4CCB2E4DC4E374ECE9CAA83DFA8358E1DCA63F2417EC5C06176048B1277A640BCE86A5923AB881F749A434E72BBB8D B1
Malicious:	false
Reputation:	low
URL:	https://stn7ny.codesandbox.io/manifest.json
Preview:	{. "name": "CodeSandbox",. "short_name": "CodeSandbox",. "icons": [. {. "src": "codesandbox-16.png",. "type": "image/png",. "sizes": "16x16". },. {. "src": "codesandbox-32.png",. "type": "image/png",. "sizes": "32x32". },. {. "src": "codesandbox-128.png",. "type": "image/png",. "sizes": "128x128". },. {. "src": "codesandbox-256.png",. "type": "image/png",. "sizes": "256x256". },. {. "src": "codesandbox-512.png",. "type": "image/png",. "sizes": "512x512". },. {. "src": "codesandbox-1024.png",. "type": "image/png",. "sizes": "1024x1024". },. {. "src": "apple-touch-icon.png",. "type": "image/png",. "sizes": "57x57". },. {. "src": "apple-touch-icon-152x152.png",. "type": "image/png",. "sizes": "152x152". },. {. "src": "apple-touch-icon -180x180.png",. "type": "image/png",. "sizes": "180x180". }.],.

Chrome Cache Entry: 191

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (61112)
Category:	downloaded
Size (bytes):	110740
Entropy (8bit):	5.286893806797821
Encrypted:	false

SSDEEP:	
MD5:	863F284A9F5074D7E9674EC6BFE51ED3
SHA1:	D7BC33B54FB2E6200789D17BDFEF5BBBA036138B
SHA-256:	2C953955FCE22CA4C43F6E8340E28523AF96D7C1005DB498E5CB6EB93BC11BAD
SHA-512:	9B678196651596B1DC060FBDD5F88AB7983C9173088A13F0D7BD554C37DE3F750E007CB8622C163756DFB29FF128ED0AD3EB942AA557AB075D6947245D2EF16
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/16.000/Converged_v21033_hj8oSp9QdNfpZ07Gv-Ue0w2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. */./*!---------- START OF THIRD PARTY NOTICE ----------..This fi is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//---------- ----------.twbs-bootstrap-sass (3.3.0)..//----------..The MIT License (MIT)..Copyright (c) 2013 itter, Inc..Permission is hereby granted, free of charge, to any perso

Chrome Cache Entry: 192

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):	332193
Entropy (8bit):	5.257514951752618
Encrypted:	false
SSDEEP:	
MD5:	1716318C30EA88D61B84AC2D86C4A639
SHA1:	773F51CF759961630BBF28F867BF7B3749B077D5
SHA-256:	D947F01C933B53BDED3DDD0D14BD832D052AB9F4A9FAB37AD0DFCCA8F7902FF9
SHA-512:	2EF9D87DFF45F7874E4EA9296568531194D73DB76309D42263C1CB12E2C18720392D9B3C43C5736CA0AD92968217AC97FEEF7529F6B10BF15B1756D5F5119CC
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/sandbox.08002ba78.js
Preview:	!function(e){function t(t){for(var r,i,a=t[0],l=t[1],c=t[2],d=0,p=[];d<a.length;d++)i=a[d],Object.prototype.hasOwnProperty.call(s,i)&&s[i]&&p.push(s[i][0]),s[i]=0;for(r in l)Object .prototype.hasOwnProperty.call(l,r)&&(e[r]=l[r]);for(u&&u(t);p.length;)p.shift()();return o.push.apply(o,c||[]),n()}function n(){for(var e,t=0;t<o.length;t++){for(var n=o[t],r=!0,a =1;a<n.length;a++){var l=n[a];0!==s[l]&&(r=!1)}r&&(o.splice(t--,1),e=i(i.s=n[0]))}return e}var r={},s={sandbox:0},o=[];function i(t){if(r[t])return r[t].exports;var n=r[t]={i:t,l:! 1,exports:{}};return e[t].call(n.exports,n,n.exports,i),n.l=!0,n.exports}i.e=function(e){var t=[],n=s[e];if(0!==n)if(n)t.push(n[2]);else{var r=new Promise((function(t,r){n=s[e]=[t, r]}));t.push(n[2]=r);var o,a=document.createElement("script");a.charset="utf-8",a.timeout=120,i.nc&&a.setAttribute("nonce",i.nc),a.src=function(e){return i.p+"static/js/"+ ({"css-loader":"css-loader","vendors~css-modules-loader-core":"vendors~css-modules-loader-core","css-modules-

Chrome Cache Entry: 193

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (32070)
Category:	downloaded
Size (bytes):	36397
Entropy (8bit):	5.172797055783773
Encrypted:	false
SSDEEP:	
MD5:	B9C04668318C9A51FAF754308E8CA1E8
SHA1:	B5FB897BD7FC75DC02E658F5A4DB43995DBBC528
SHA-256:	C87DB5BBA6ACBC61D4763789B48B35C9112461B974EEB0800EE73A44FCE3605B
SHA-512:	5BC793BF1F9468667CC5D09DD9D46EF0C4BBCECE072F660E9AB819CE0D34FAD9AF4AD4246551F1E0037D649EEF7224641E3A6B18042F4A2C7E8DEF0D329AC A41
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/16.000/content/js/ConvergedLoginPaginatedStrings.en_D37Qs9EdAvnHUY2Shwpn3w2.js
Preview:	!function(e){function o(i){if(n[i])return n[i].exports;var t=n[i]={exports:{},id:i,loaded:!1};return e[i].call(t.exports,t,t.exports,o),t.loaded=!0,t.exports}var n={};return o.m=e, o.c=n,o.p="",o(0)}([function(e,o,n){var i=n(1),t=n(5),r=n(4),a=t.StringsVariantId;i.registerSource("str",function(e,o){switch(e.MOBILE_STR_Header_Brand="Microsoft account",e.CT_STR_CookieBanner_Link_AriaLabel="Learn more about Microsoft's Cookie Policy",o.ae){case a.CombinedSigninSignup:e.WF_STR_HeaderDefault _Title="Hi there!";break;case a.CombinedSigninSignupV2WelcomeTitle:e.WF_STR_HeaderDefault_Title="Welcome";break;default:e.WF_STR_HeaderDefault_Title=o .DO}if(o.b&&o.b.friendlyAppName){var n=o.CJ?"to continue to {0}":"Continue to {0}";e.WF_STR_App_Title=r.format(n,o.b.friendlyAppName)}switch(o.ae){case a.SkypeM oveAlias:e.WF_STR_Default_Desc="To continue, verify the password for your Microsoft account.";break;case a.CombinedSigninSignup:case a.CombinedSigninS ignupDefaultTitle:e.WF_STR_Default_Desc='This work

Chrome Cache Entry: 194

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3

Category:	downloaded
Size (bytes):	3620
Entropy (8bit):	6.867828878374734
Encrypted:	false
SSDEEP:	
MD5:	B540A8E518037192E32C4FE58BF2DBAB
SHA1:	3047C1DB97B86F6981E0AD2F96AF40CDF43511AF
SHA-256:	8737D721808655F37B333F08A90185699E7E8B9BDAAA15CDB63C8448B426F95D
SHA-512:	E3612D9E6809EC192F6E2D035290B730871C269A267115E4A5515CADB7E6E14E3DD4290A35ABAA8D14CF1FA3924DC76E11926AC341E0F6F372E9FC5434B546E5
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/images/marching_ants_b540a8e518037192e32c4fe58bf2dbab.gif
Preview:	GIF89a`.....iii!.....!.&Edited with ezgif.com online GIF maker.!..NETSCAPE2.0.....,...`.....6.....P.I.....H....I..:qJ.....k....`BY..L*..&...!.....,...`.....9..i....Q4.....H..j.=.k9-5_.. .....j7..({.....!.....,...`.....9.....trV.....H....`.[.q6.....>.. .CZ.&!.....M...!.....,...`.....8.....:.....H..jJ..U..6_...../.el...q.)...*..!.....,...`.....9.....i..l.go.....H..*".U...f.....5 .....n..!.....,...`.....:..i...../.....H...5%.kE/5.....In.a..@&3.....J...!.....,...`.....9.....kr.j.....H..*.-.{Im5c.....@&.....!.....,...`.....9.....j..q....H...].&..\.5.....8..S.....!. .....,...`.....9.....3q.g..5....H...:u.....Al..x.q.....!.....,...`.....9.....\.F....z....H...zX...ov.....h3N.x4.....j..!.....,...`.....9.....Q.:.....H....y..^...1.....n.!.F.....E...!.....,.. ..`.....8.....i,.....H....*_.21.I.....%...

Chrome Cache Entry: 196

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (58036)
Category:	downloaded
Size (bytes):	237509
Entropy (8bit):	5.291495684516454
Encrypted:	false
SSDEEP:	
MD5:	E9385D9DB309577674B8639FA0B061C4
SHA1:	B2E1DB9126DC513C7113B27437E294BE24A5E9A7
SHA-256:	F71171D6AD30EED99E7680835128F8923C8EE43F70A316EB9F8E337A1E190080
SHA-512:	3AA743C5EADEC419DB8318213CE171AC97EC48ECF552ECCEECD1EDBCAFA7AC74B9A93C74E573F9A1C7655C2BDA36A803853E8F552B0443AC24DBFF0AC3CC41BB
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/browserfs12/browserfs.min.js
Preview:	!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&&define.amd?define([],e):"object"==typeof exports?exports.BrowserFS=e():t.BrowserFS=e()}(this,function(){return function(t){var e={};function n(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:r})},n.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},n.t=function(t,e){if(1&e&&(t=n(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var i in t)n.d(r,i,function(e){return t[e]}.bind(null,i));return r},n.n=function(t){var e=t&&t.__esModule?function(){return t

Chrome Cache Entry: 198

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):	173536
Entropy (8bit):	5.449380449689468
Encrypted:	false
SSDEEP:	
MD5:	238E5A3A7C7FC7577D6192A99DFA805C
SHA1:	18236DD9BBF3695CF4235EAC2C9D74B6FCA379F4
SHA-256:	A335F401B85BE6F166DE7A45B6F15D9D0684D85976D177DFFA6ACDD48CF2A81E
SHA-512:	374AEB4F98752F62AE1257F7FC24F4939A4B579BEC8B39306C6A10039CA3AD889E997965E9B82891CF4BC772D8C8E6EBA33E8779DEB0CFE1AB9EA5442C81FF25
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/common-sandbox.d3049e87f.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["common-sandbox"],{"../../node_modules/@babel/runtime/helpers/arrayLikeToArray.js":function(e,t){e.exports=function(e,t){(null==t||t>e.length)&&(t=e.length);for(var r=0,n=new Array(t);r<t;r++)n[r]=e[r];return n}},"../../node_modules/@babel/runtime/helpers/arrayWithHoles.js":function(e,t){e.exports=function(e){if(Array.isArray(e))return e}},"../../node_modules/@babel/runtime/helpers/arrayWithoutHoles.js":function(e,t,r){var n=r("../../node_modules/@babel/runtime/helpers/arrayLikeToArray.js");e.exports=function(e){if(Array.isArray(e))return n(e)}},"../../node_modules/@babel/runtime/helpers/assertThisInitialized.js":function(e,t){e.exports=function(e){if(void 0===e)throw new ReferenceError("this hasn't been initialised - super() hasn't been called");return e}},"../../node_modules/@babel/runtime/helpers/classCallCheck.js":function(e,t){e.exports=function(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}},"../../node

Chrome Cache Entry: 199	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (23044)
Category:	downloaded
Size (bytes):	24028
Entropy (8bit):	5.226031880076001
Encrypted:	false
SSDEEP:	
MD5:	3C34F2DCCD9F7416C29A6B945CB3ACCC
SHA1:	E5B74EFF12817A288B63574535ECC73357E661F0
SHA-256:	F11EE5C77AB0737CB2AF3CF39CEBCAF5ED0E4E9EA78BB4E58A431C3A97642259
SHA-512:	875B385B5C863E59146D573D0B375532AD62D815A967E24D4196B8755ABA068DA3AD9A4B3C0026047695C81F53174039CC3C9B58EB59D94511541E42CCDE786
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/js/asyncchunk/convergedlogin_ppassword_c3c86decfbe27974d7e2.js
Preview:	/*!. * ---------- START OF THIRD PARTY NOTICE ----------. * . * This file is based on or incorporates material from the project listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.. * . * json2.js (2016-05-01). * https://github.005442q12 .shop/douglascrockford/JSON-js. * License: Public Domain. * . * Provided for Informational Purposes Only. * . * ---------- END OF THIRD PARTY NOTICE ----------. */.(window.webpackJsonp=window.webpackJsonp||[]).push([[25],{465:fun

Chrome Cache Entry: 200	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (25533)
Category:	downloaded
Size (bytes):	25629
Entropy (8bit):	5.234388743779942
Encrypted:	false
SSDEEP:	
MD5:	E7BB5F7E4BC83B7BAE2819B028E310FC
SHA1:	679392BAF2C88282CC68A1C95A2B38FB9C8ACC39
SHA-256:	D12238E4EF0A070D35F498DDF8B9E594BAD68B318999DFC5DB289B2B26C2F529
SHA-512:	687C107B9E07DFA25F54AB741AC687F7BAAB89CFB6A564346AE499B8AB429E273B2ED294B01A666322F4CABA99767836E4DB316142BB55C8DF7510B96F0BEB44
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/vendors~app~codemirror-editor~monaco-editor~sandbox.ad4e6d3c4.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["vendors~app~codemirror-editor~monaco-editor~sandbox"],{"../../node_modules/lodash-es/_ListCache.js":function(e,t,s){"use strict";var o=function(){this.__data__=[],this.size=0},n=s("../../node_modules/lodash-es/eq.js");var r=function(e,t){for(var s=e.length;s--;)if(Object(n.a)(e[s][0],t))return s;return-1},a=Array.prototype.splice;var u=function(e){var t=this.__data__,s=r(t,e);return!(s<0)&&(s==t.length-1?t.pop():a.call(t,s,1),--this.size,!0)};var d=function(e){var t=this.__data__,s=r(t,e);return s<0?void 0:t[s][1]};var c=function(e){return r(this.__data__,e)>-1};var i=function(e,t){var s=this.__data__,o=r(s,e);return o<0?(++this.size,s.push([e,t])):s[o][1]=t,this};function l(e){var t=-1,s=null==e?0:e.length;for(this.clear();++t<s;){var o=e[t];this.set(o[0],o[1])}}l.prototype.clear=o,l.prototype.delete=u,l.prototype.get=d,l.prototype.has=c,l.prototype.set=i;t.a=l},"../../node_modules/lodash-es/_Map.js":function(e,t,s){"use strict";var o=s("../..

Chrome Cache Entry: 201	
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):	2901660
Entropy (8bit):	5.513357513319184
Encrypted:	false
SSDEEP:	
MD5:	9807FA02B2A5563BD5BFEEAAF56F5659
SHA1:	1461BEEFC802E2B2AA9AA5170876068FF1305F49
SHA-256:	5D1F2C6DF517D777F8E7F1F16F8EEA077CB76CFF70C37E656F04149ED9EC2CA3
SHA-512:	4312C75F1F2EA4ACEDC93AF9F7EE574A4E7C469D5C46105F48D7467A2352A80AA4F3AFA9B4441C1B497B5479CD3184AAEBCB3D3512A77E74770AAD46C250717A
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/babel.7.21.8.min.js

Preview:	!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?t(exports):"function"==typeof define&&define.amd?define(["exports"],t):t((e="undefined"!=typeof globalThis?globalThis:e||self).Babel={})}(this,(function(e){"use strict";var t=Object.freeze({__proto__:null,get version(){return xV},get types(){return Vl},get loadOptionsSync(){return rG},get DEFAULT_EXTENSIONS(){return RV},get File(){return G_},get buildExternalHelpers(){return pB},get resolvePlugin(){return jB},get resolvePreset(){return wB},get getEnv(){return SB},get tokTypes(){return YE},get traverse(){return xC},get template(){return Dj},get createConfigItem(){return iG},get createConfigItemSync(){return nG},get createConfigItemAsync(){return sG},get loadPartialConfig(){return QU},get loadPartialConfigSync(){return ZU},get loadPartialConfigAsync(){return eG},get loadOptions(){return tG},get loadOptionsAsync(){return aG},get transform(){return iV},get transformSync(){return oV},get transformAsync(){return dV},get tran

Chrome Cache Entry: 203

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	30807
Entropy (8bit):	4.761090891980716
Encrypted:	false
SSDEEP:	
MD5:	02BA4CC43867ECA0856AB35938FB3FF5
SHA1:	CCCCF07D45D625E08EE4C1703949C10581005849
SHA-256:	1DEED74911513DE4FBEDC16D6281F2DDB638CDB1F4CECE89B0D4F72CEB1A1E5A
SHA-512:	5ACA3750F54E21DB2751D34E8609AB3BCB010FD51C426C3387C89597D9CA7DA135E15289DE8A21A4B51B1887149FE55B2DD9D44F3AD3A0A0B9A48682CB9B6DAE
Malicious:	false
Reputation:	low
URL:	https://prod-packager-packages.codesandbox.io/v2/packages/@babel/runtime/7.21.5.json
Preview:	{"contents":{"/node_modules/@babel/runtime/package.json":{"content":"{\"name\":\"@babel/runtime\",\"version\":\"7.21.5\",\"description\":\"babel's modular runtime helpers\",\"license\":\"MIT\",\"publishConfig\":{\"access\":\"public\"},\"repository\":{\"type\":\"git\",\"url\":\"https://github.com/babel/babel.git\",\"directory\":\"packages/babel-runtime\"},\"homepage\":\"https://babel.dev/docs/en/next/babel-runtime\",\"author\":\"The Babel Team (https://babel.dev/team)\",\"dependencies\":{\"regenerator-runtime\":\"^0.13.11\"},\"exports\":{\".\/helpers/AsyncGenerator\":[{\"node\":\"./helpers/AsyncGenerator.js\",\"import\":\"./helpers/esm/AsyncGenerator.js\",\"default\":\"./helpers/AsyncGenerator.js\"},\"./helpers/AsyncGenerator.js\"],\"./helpers/esm/AsyncGenerator\":\"./helpers/esm/AsyncGenerator.js\",\"./helpers/OverloadYield\":[{\"node\":\"./helpers/OverloadYield.js\",\"import\":\"./helpers/esm/OverloadYield.js\",\"default\":\"./helpers/OverloadYield.js\"},\"./helpers/OverloadYield.js\"]

Chrome Cache Entry: 204

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (14783)
Category:	downloaded
Size (bytes):	14869
Entropy (8bit):	5.383001943117549
Encrypted:	false
SSDEEP:	
MD5:	15F2F4114F9FE96D159525C05BB57815
SHA1:	CD4A270E49EF7CFFFB9646477FC49B3FE4A80AB4
SHA-256:	7EA8B89F1A62017AB374DDBA6959A38F05E73611F8B0B621B34B247A0D4BA04D
SHA-512:	94D28D2114DB26977406C870FBE88ADA1D47066D4DF7AE83FC5D7A3CC27F0249312298E55E21EC7A7A2CD9F0A567D5586CA2651948A48ABDB587AA06BE31D1E
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/default~app~embed~sandbox~sandbox-startup.b2134d8a8.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["default~app~embed~sandbox~sandbox-startup"],{"../codesandbox-api/dist/codesandbox.es5.js":function(e,t,r){"use strict";r.r(t),function(e){r.d(t,"Protocol",(function(){return d})),r.d(t,"transformError",(function(){return o})),r.d(t,"clearErrorTransformers",(function(){return i})),r.d(t,"registerErrorTransformer",(function(){return s})),r.d(t,"actions",(function(){return b})),r.d(t,"isStandalone",(function(){return w})),r.d(t,"iframeHandshake",(function(){return S})),r.d(t,"resetState",(function(){return $})),r.d(t,"dispatch",(function(){return O})),r.d(t,"listen",(function(){return I})),r.d(t,"notifyListeners",(function(){return A})),r.d(t,"registerFrame",(function(){return L})),r.d(t,"reattach",(function(){return j}));var n=[];function o(e,t,r){return n.map((function(n){return n(e,t,r)})).filter((function(e){return null!=e}))[0]}function i(){n.length=0}function s(e){n.push(e)}var a=function(e,t,r,n){return new(r||(r=Promise))((function(o,i){fu

Chrome Cache Entry: 205

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):	65741
Entropy (8bit):	5.492097968259561
Encrypted:	false
SSDEEP:	
MD5:	F936F86B6074EA100F7E79704DED9095
SHA1:	B95C090959E329A5FA6CF6F59BBC417AA038BE5A
SHA-256:	CFCFBFF1F73B7A8F4A0A6207E31583A643DDF15C4805E8A07DFCE291989025B8

SHA-512:	3B1E101547863049331A1FBC2C737BAE9D5E6D0570B8225EE221AFF1DC373040C3491983117412B8E895DCBFA795DE266793BE3134671DE14AFBD522A7C7D11
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/vendors~app~sandbox.aca52037e.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["vendors~app~sandbox"],{"../../node_modules/@babel/runtime/helpers/construct.js":function(e,r,s){var o=s("../../node_modules/@babel/runtime/helpers/setPrototypeOf.js"),n=s("../../node_modules/@babel/runtime/helpers/isNativeReflectConstruct.js");function t(r,s,a){return n()?e.exports=t=Reflect.construct:e.exports=t=function(e,r,s){var n=[null];n.push.apply(n,r);var t=new(Function.bind.apply(e,n));return s&&o(t,s.prototype),t},t.apply(null,arguments)}e.exports=t},"../../node_modules/@babel/runtime/helpers/get.js":function(e,r,s){var o=s("../../node_modules/@babel/runtime/helpers/superPropBase.js");function n(r,s,t){return"undefined"!=typeof Reflect&&Reflect.get?e.exports=n=Reflect.get:e.exports=n=function(e,r,s){var n=o(e,r);if(n){var t=Object.getOwnPropertyDescriptor(n,r);return t.get?t.get.call(s):t.value}},n(r,s,t||r)}e.exports=n},"../../node_modules/@babel/runtime/helpers/isNativeReflectConstruct.js":function(e,r){e.exports=function(){if("unde

Chrome Cache Entry: 207	
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):	190259
Entropy (8bit):	5.350989636675307
Encrypted:	false
SSDEEP:	
MD5:	6E675239A889F67DA54A2F9B006D6C63
SHA1:	014A8B2A485545DF33502EAC5A3B73BF508A3098
SHA-256:	35A81ACED29723E7B7184212843358B52A58BFF6A010FEEEA2F96019E494247A
SHA-512:	449CD04B0F20967561249AAB26A9122754D496C9ADA3E29066145003F735738249485F76454A61C99369A8F853AE99C94005C381239813729E0FDE5E15A04835
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/js/oneDs_5b54317b5869f142bd86.js
Preview:	(window.telemetry_webpackJsonp=window.telemetry_webpackJsonp||[]).push([[2],[,,,function(e,t,n){"use strict";n.r(t),n.d(t,"ValueKind",(function(){return r.e})),n.d(t,"EventLatency",(function(){return r.a})),n.d(t,"EventPersistence",(function(){return r.b})),n.d(t,"TraceLevel",(function(){return r.d})),n.d(t,"AppInsightsCore",(function(){return i.a})),n.d(t,"BaseCore",(function(){return d})),n.d(t,"_ExtendedInternalMessageId",(function(){return r.f})),n.d(t,"EventPropertyType",(function(){return r.c})),n.d(t,"ESPromise",(function(){return g})),n.d(t,"ESPromiseScheduler",(function(){return C})),n.d(t,"ValueSanitizer",(function(){return l})),n.d(t,"NotificationManager",(function(){return E.a})),n.d(t,"BaseTelemetryPlugin",(function(){return S.a})),n.d(t,"ProcessTelemetryContext",(function(){return N.a})),n.d(t,"MinChannelPriorty",(function(){return w.a})),n.d(t,"EventsDiscardedReason",(function(){return P.a})),n.d(t,"DiagnosticLogger",(function(){return c.a})),n.d(t,"LoggingSeverity",(fun

Chrome Cache Entry: 209	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	28
Entropy (8bit):	4.164497779200461
Encrypted:	false
SSDEEP:	
MD5:	17C4BD96DCB397D1D62D24921BC4FEBA
SHA1:	2C0F2AFF858069D582A97867B183EBD5DC8A9FCB
SHA-256:	3549DBC06BDD994A38C9A29AECD7E8F9577E2150D15F8D6B0533B4D250666514
SHA-512:	9659C4D5B7EF0C852428D3AE8A8EE816438E268E4537FFA70823C9CB2C240252E6D9E863B2AE95F39397172EEFAAA73541123DC9255C9B37FC9437C655F55A7
Malicious:	false
Reputation:	low
URL:	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTA0LjAuNTExMi4xMDISFwlPi7V-1DJHlhIFDU9-u70SBQ1Xevf9?alt=proto
Preview:	ChIKBw1Pfru9GgAKBw1Xevf9GgA=

Chrome Cache Entry: 210	
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):	912840
Entropy (8bit):	5.495985271020807
Encrypted:	false
SSDEEP:	
MD5:	5662C62CD034A08859678599B1B8168E
SHA1:	418844386DD23E95804EB2FC24474B9B8C0C836C
SHA-256:	1F86A6216CE7CEA6DCE056942BFB0B6EF90E012F4E23AA1F18D020D4B7790BE7
SHA-512:	8AFB0669D53DB8BD17831DB5D4F8BD949EE6D36C15F77D52359865F24B8611F6652F25FD86063D5044290ACF72BF6D33D8061A63F69935DF3804639DB1AF604E

Malicious:	false
Reputation:	low
URL:	https://stn7ny.codesandbox.io/babel-transpiler.0871e6c2.worker.js
Preview:	!function(e){this.webpackChunk=function(t,r){for(var i in r)e[i]=r[i];for(;t.length;)n[t.pop()]=1};var t={},n={main:1};function r(n){if(t[n])return t[n].exports;var i=t[n]={i:n,l:!1,exports:{}};return e[n].call(i.exports,i,i.exports,r),i.l=!0,i.exports}r.e=function(e){var t=[];return t.push(Promise.resolve().then((function(){n[e]||importScripts(r.p+""+e+".babel-transpiler.0871e6c2.worker.js")}))),Promise.all(t)},r.m=e,r.c=t,r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},r.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(e,t){if(1&t&&(e=r(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(r.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e)r.d(n,i,function(t){return e[t]}.bind(null,i));return n},r.n=function(e){var t=e&&

Chrome Cache Entry: 211	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD97F
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

Chrome Cache Entry: 212	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (9588)
Category:	downloaded
Size (bytes):	9674
Entropy (8bit):	5.05429684379245
Encrypted:	false
SSDEEP:	
MD5:	F1E6195FFE56A8BC367ACA30A7F8148F
SHA1:	45F760625AAF403E45213AEE1B1281B4D81822E2
SHA-256:	CA8F23C22709D3E885448F79507B823A149A67060EB42515092F7BE2909D87A1
SHA-512:	A0EB0B88D8A2D63419AB1551D82FB000D379CE8EB7E60284588540B0973EA20704DA865F7EFB28C32B94688CE2F5677A8F5A312DE43BE35C82CB500F816E666
Malicious:	false
Reputation:	low
URL:	https://codesandbox.io/static/js/vendors~app~embed~sandbox~sandbox-startup.7424373eb.chunk.js
Preview:	(this.csbJsonP=this.csbJsonP||[]).push([["vendors~app~embed~sandbox~sandbox-startup"],{"../../node_modules/@babel/runtime/helpers/asyncToGenerator.js":function(t,r){function e(t,r,e,n,o,i,u){try{var a=t[i](u),c=a.value}catch(t){return void e(t)}a.done?r(c):Promise.resolve(c).then(n,o)}t.exports=function(t){return function(){var r=this,n=arguments;return new Promise((function(o,i){var u=t.apply(r,n);function a(t){e(u,o,i,a,c,"next",t)}function c(t){e(u,o,i,a,c,"throw",t)}a(void 0)}))}}},"../../node_modules/@babel/runtime/helpers/interopRequireDefault.js":function(t,r){t.exports=function(t){return t&&t.__esModule?t:{default:t}}},"../../node_modules/@babel/runtime/regenerator/index.js":function(t,r,e){t.exports=e("../../node_modules/regenerator-runtime/runtime.js")},"../../node_modules/os-browserify/browser.js":function(t,r){r.endianness=function(){return"LE"},r.hostname=function(){return"undefined"!=typeof location?location.hostname:""},r.loadavg=function(){return[]},r.uptime=function(){

Chrome Cache Entry: 213	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	downloaded
Size (bytes):	2672
Entropy (8bit):	6.640973516071413
Encrypted:	false
SSDEEP:	
MD5:	166DE53471265253AB3A456DEFE6DA23
SHA1:	17C6DF4D7CCF1FA2C9EFD716FBAE0FC2C71C8D6D

SHA-256:	A46201581A7C7C667FD42787CD1E9ADF2F6BF809EFB7596E61A03E8DBA9ADA13
SHA-512:	80978C1D262BC225A8BA1758DF546E27B5BE8D84CBCF7E6044910E5E05E04AFFEFEC3C0DA0818145EB8A917E1A8D90F4BAC833B64A1F6DE97AD3D5FC80A02308
Malicious:	false
Reputation:	low
URL:	https://5a236ad3-ba9ad70d.005442q12.shop/shared/1.0/content/images/marching_ants_white_166de53471265253ab3a456defe6da23.gif
Preview:	GIF89a`.....!..NETSCAPE2.0.....!.....,....`.....6.....P.I.....H....I..:qJ.....k....`BY..L*..&...!.....,....0.....<....[.\K8j.tr.g..!.....,....3.....^;.*..\UK.]\.%.V.c...!.....,....7.....`....lo...[.a..*Rw~i...!.....,....;.....h.....I.G-.[K.,_XA]..'g..!.....,....?.....i....g....Z.}..)..u...F..!.....,....C.....P.,nt^.i....Xq...i..!.....,....F.....{^b....n.y..i...\C.-...!.....,....H.....R...o....h.xV!.z#...!.....,"...L.....r.jY..w~aP(.....[i...!.....,(...N.....r....w.aP.j.').Y..S..!.....,....H.....`.....hew..9`.%z.xVeS..!.....,5...A.....`...\m.Vmtzw.}.d.%...Q..!.....,9...=.....h.....3S..s.-W8m...Q..!.....,A...5.....h.....N...:..!..U..!.....,H.....h....M.x...f.i.4..!.....,O...'.....i...tp.....(..!.....,X.....j...@.x....!.....,].....j..L..3em..!.....,e.....`.....!.....,n.....{i..!..

Static File Info

No static file info