ID: 830993
Cookbook: browseurl.jbs
Time: 22:56:30
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

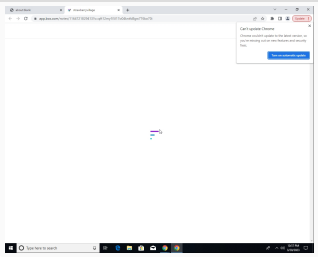
Windows Analysis Report

https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i

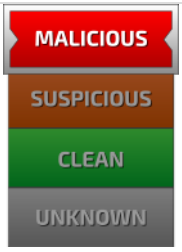
Overview

General Information

Sample URL:	http://https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i
Analysis ID:	830993
Infos:	



Detection



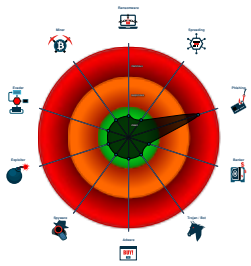
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- HTML body contains low number of …
- Invalid T&C link found
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5072 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1316 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1828 --field-trial-handle=1768,i,15355743440405815616,15119586194272472126,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2344 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
dropped/chromecache_167	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

HTML

Source	Rule	Description	Author	Strings
94194.4.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
94194.6.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Phishing

Yara detected HtmlPhish10

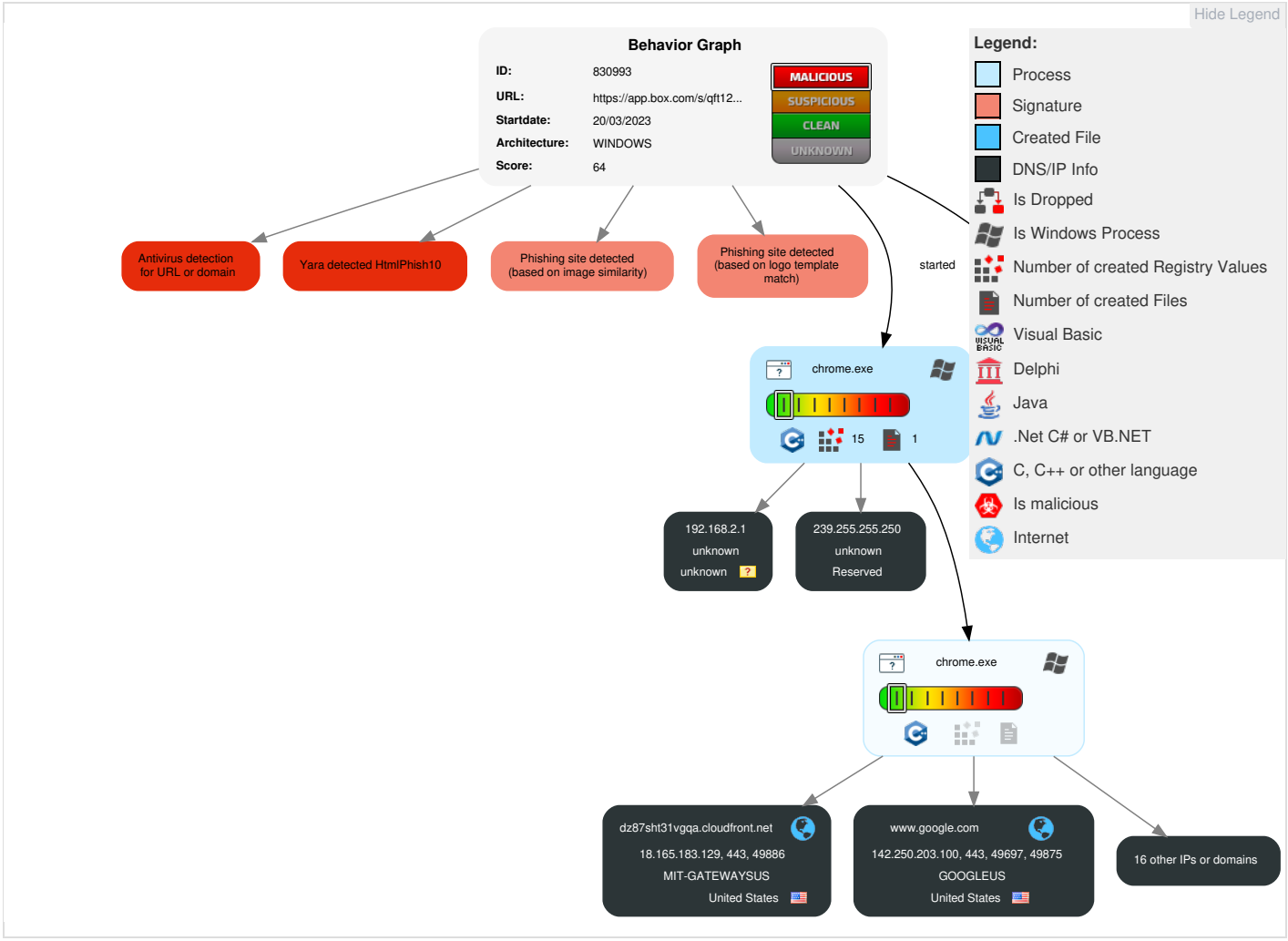
Phishing site detected (based on logo template match)

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	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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

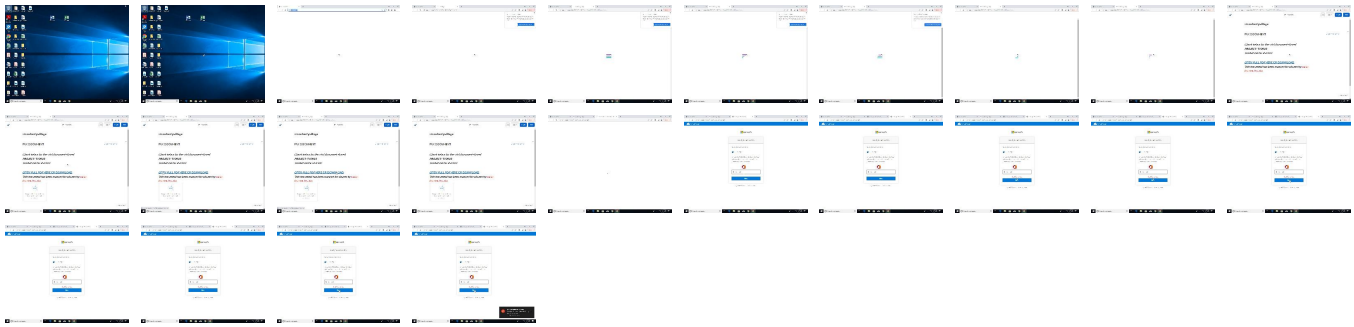
Behavior Graph

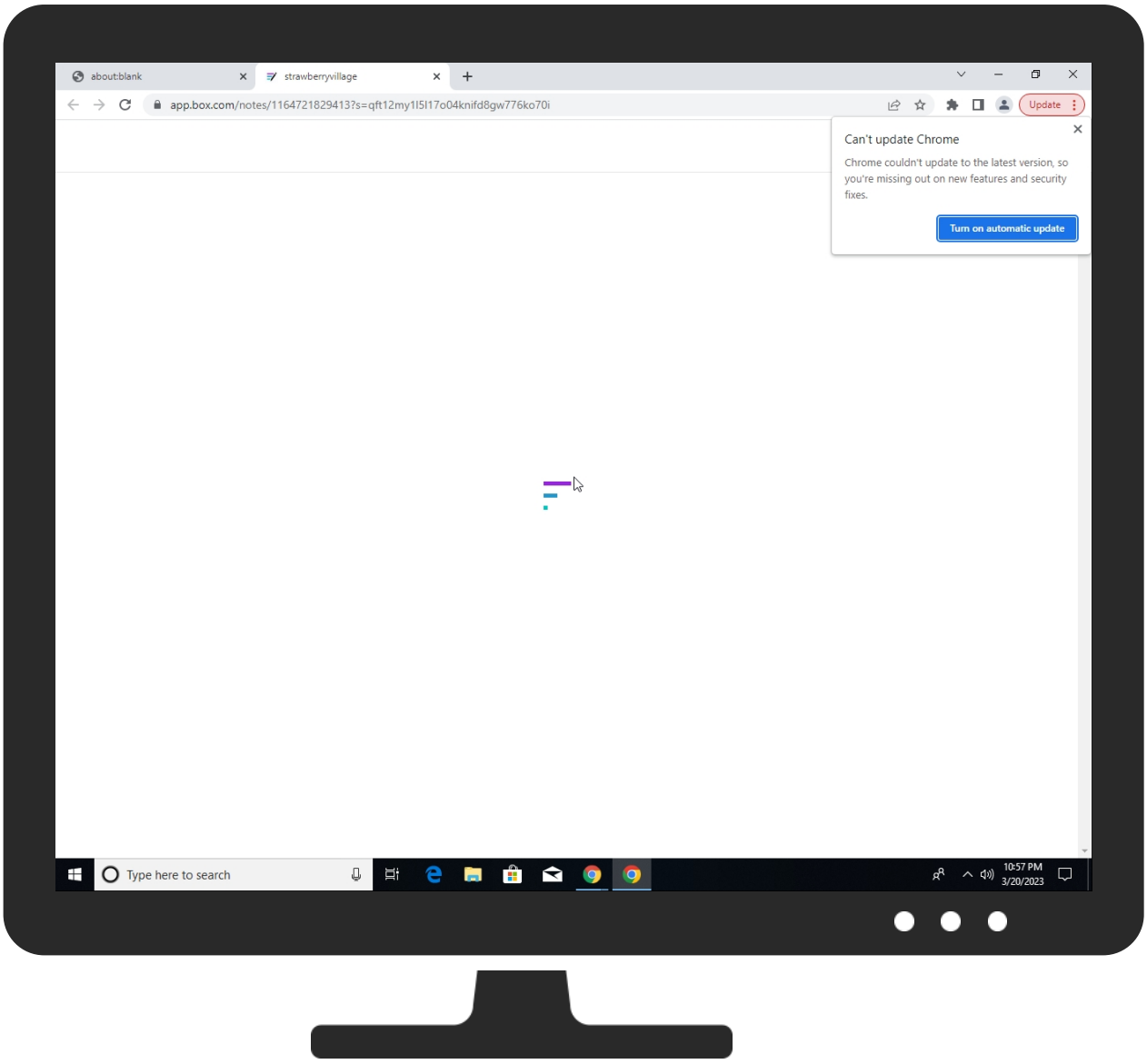


Screenshots

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://https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i	0%	Avira URL Cloud	safe	
http://https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i	1%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://app.box.com/notes/1164721829413?s=qft12my1l5l17o04knifd8gw776ko70i	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://https://faxmail-secondary.z13.web.core.windows.net/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://notes.services.box.com/p/note?fileId=1164721829413&hostname=app.box.com&sharedLink=https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://youngarsmfg.com/faxmail/postoo.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
auth.split.io	35.170.228.5	true	false		high
accounts.google.com	142.250.203.109	true	false		high
notes.services.box.com	74.112.186.144	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
app.box.com	74.112.186.144	true	false		high
client-log.box.com	74.112.186.144	true	false		high
dz87sht31vgqa.cloudfront.net	18.165.183.129	true	false		high
sdk.split.io	unknown	unknown	false		high
cdn01.boxcdn.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
streaming.split.io	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://notes.services.box.com/client_log	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nUa	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=websocket&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11pEj&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12BrD&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11qbU&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11zUs&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11_GT&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS1212l&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11_GR&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12A3U&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/box-image?encoding=base64&fileId=1164711816928&fileName=Box%20Notes%20Image%202023-03-14%2021.15.17.png&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2F821u4wbadx46bwm98ch1k57gcclzy6zt&viewContext=inline	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=websocket&sid=IpvWMe6y-UCxux37ALr5	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12BrF&sid=FJ53pnQpy7l_zAfJALr7	false		high

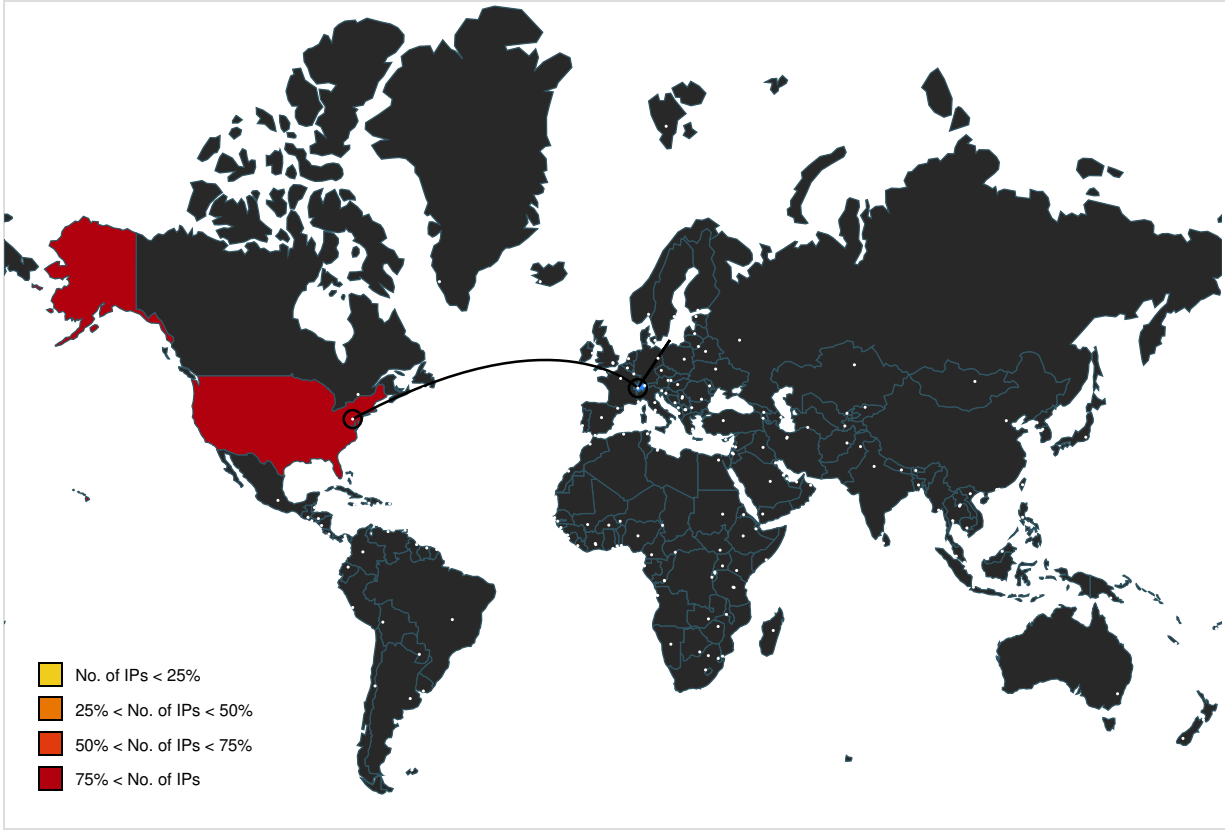
Name	Malicious	Antivirus Detection	Reputation
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11o1h&sid=lpvWMe6y-UCxux37ALr5	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS1212X&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/p/note?fileId=1164721829413&hostname=app.box.com&sharedLink=https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11opk	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS122q3&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS124ku&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11ou9&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS128I0&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12A3X&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12DdH&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11u9U&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11ou7&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11qbV&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nYq&sid=lpvWMe6y-UCxux37ALr5	false		high
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-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11piq&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11xjD&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nup&sid=lpvWMe6y-UCxux37ALr5	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12DdG&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/box-image?fileId=1164711816928&fileName=Box%20Notes%20Image%202023-03-14%2021.15.17.png&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2F821u4wbadx46bwm98ch1k57gcclzy6zt&viewContext=inline	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11u9c&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://client-log.box.com/analytics-events/	false		high
http://https://notes.services.box.com/app_init?authCode=&fileId=1164721829413&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2Fqft12my1l5l17o04knifd8gw776ko70i&listId=inbox&_=1679349452464	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11psM&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11ndN&sid=lpvWMe6y-UCxux37ALr5	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS126W8&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11zUv&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11ndL&sid=lpvWMe6y-UCxux37ALr5	false		high
http://https://notes.services.box.com/clientSocketConnectionInfo?fileId=1164721829413&_=1679349452465	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	false		high
http://https://app.box.com/notes/1164721829413?s=qft12my1l5l17o04knifd8gw776ko70i	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high

Name	Malicious	Antivirus Detection	Reputation
http://https://notes.services.box.com/p/note?fileId=1164721829413&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2Fqft12my1l5l17o04knifd8gw776ko70i&hostname=app.box.com	false		high
http://https://app.box.com/notes/1164721829413?s=qft12my1l5l17o04knifd8gw776ko70i	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11sN_&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS124km&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11p_u&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11vxR&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11xjH&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://auth.split.io/api/v2/auth?users=key	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS126WP&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nue&sid=lpvWMe6y-UCxux37ALr5	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11psr&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS122q1&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nYg&sid=lpvWMe6y-UCxux37ALr5	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11pEh&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11sN-&sid=FJ53pnQpy7l_zAfJALr7	false		high
http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS128Hz&sid=FJ53pnQpy7l_zAfJALr7	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	chromecache_167.1.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	chromecache_224.1.dr, chromecache_181.1.dr	false		high
http://opensource.org/licenses/MIT).	chromecache_220.1.dr	false		high
http://https://app.box.com/s/821u4wbadx46bwm98ch1k57gcclzy6zt	chromecache_194.1.dr, chromecache_223.1.dr	false		high
http://https://youngarsmfg.com/faxmail/postoo.php	chromecache_167.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://getbootstrap.com/)	chromecache_224.1.dr	false		high
http://https://getbootstrap.com)	chromecache_181.1.dr, chromecache_190.1.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	chromecache_224.1.dr, chromecache_181.1.dr, chromecache_190.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.112.186.144	notes.services.box.com	United States		33011	BOXNETUS	false
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
18.165.183.129	dz87sht31vgqa.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
35.170.228.5	auth.split.io	United States		14618	AMAZON-AESUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830993
Start date and time:	2023-03-20 22:56:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i
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:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@29/65@23/12
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://faxmail-secondary.z13.web.core.windows.net/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 104.16.74.20, 104.18.103.56, 172.217.168.10, 172.217.168.42, 172.217.168.74, 142.250.203.106, 216.58.215.234, 151.101.3.9, 151.101.67.9, 151.101.131.9, 151.101.195.9, 20.60.80.79, 152.199.19.161, 69.16.175.10, 69.16.175.42
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, cds.s5x3j6q5.hwcdn.net, spoppe-b.ec.azureedge.net, content-autofill.googleapis.com, ajax.googleapis.com, fonts.gstatic.com, ctldl.windowsupdate.com, clientservices.googleapis.com, faxmail-secondary.z13.web.core.windows.net, edgedl.me.gvt1.com, spoppe-b.azureedge.net, update.googleapis.com, web.sjc20prdstr19b.store.core.windows.net, cdn01.boxcdn.net.cdn.cloudflare.net, e3.shared.global.fastly.net, cs9.wpc.v0cdn.net
- 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

Chrome Cache Entry: 161

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS124ku&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 162

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (31952)
Category:	downloaded
Size (bytes):	48797
Entropy (8bit):	4.8072489684235995
Encrypted:	false
SSDEEP:	768:lpQ9KDQmYm1j7xS7kmObTyQW620xdxCImqCzP/XDKFjy9iwjn7nQNOSfclLQD2mV:lpQ9KDQmYm1j7xS7kmObTyQW620xdxCF
MD5:	B5307E4A0D56B62E41600E1296BF75AA
SHA1:	76B57440EFC1A382989E8BED80379D2C00FCA64B
SHA-256:	DEF6F66252A9F848DFBE00904DF6D26A4215051EC39C7CB361AAACDC2BAAD889
SHA-512:	F028F5DDFB6405838AA5DC50BD8E52F120173D4A6DF9F2197AE5ECD6BF0B1246E6B186A0453AA31D45A5CE7FFF486CD578FC6A459A48A321EA97CF2596CD7035
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/js/l10n/en-i18n_292a3b30bf4cf4524e29952b28bb684f.min.js
Preview:	!function(e){var t=function(e,t){if(isNaN(e))throw new Error("'"+e+"' isn't a number.");return e-(t||0)},n=function(e,t,n,o,r){if(e in o)return o[e];t&&(e-=t);var i=n(e,r);return i in o?o[i]:o.other},o={en:function(e,t){var n=String(e).split("."),o=!n[1],r=Number(n[0])==e,i=r&&n[0].slice(-1),u=r&&n[0].slice(-2);return t?1==i&&11!=u?"one":2==i&&12!=u?"two":3==i&&13!=u?"few":"other":1==e&&o?"one":"other"}};e.i18n={en:{"note.yes":function(e){return"Yes"},"note.no":function(e){return"No"},"note.datetime":function(e){return e.date+" at "+e.time},"note.date":function(e){return e.month+"/"+e.day+"/"+e.year},"note.date.abbreviated.noYear":function(e){return e.month+" "+e.day},"note.date.abbreviated.full":function(e){return e.month+" "+e.day+" "+e.year},"note.date.month.short.January":function(e){return"Jan"},"note.date.month.short.February":function(e){return"Feb"},"note.date.month.short.March":function(e){return"Mar"},"note.date.month.short.April":function(e){return"Apr"},"note.date.month.sho

Chrome Cache Entry: 163

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	200
Entropy (8bit):	4.757053006893356
Encrypted:	false
SSDEEP:	6:qSpPipnVNipnVNip7zKXLQVQUXLQVQUXj:qS9iBiBi9zoLi5Li5j
MD5:	476EE9F49094D8DF9E723601C0AFD54C
SHA1:	669A2662F1BB3C63DC2889848019556E940BB8C1
SHA-256:	D6325E8E8E5B4EAE02BC3EECBED3300443940CFED7BC51DC564B79AE8DE333D7
SHA-512:	08BAE76918F138CCD08D863A5E84750A5FEAD861FB65FFA89DBCBAA2923330100907E360572220F660685D1F8F7DA89922722E7CF66E2B32EC7B293BDC47E9F
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA0LjAuNTExMi44MRJBCZ8u4PYFXWUWEgUNSoWeUhIFDUqFnlISBQ0G7bv_EgUNBu27_xIFDUqFnlISBQ0G7bv_EgUNBu27_xIFDUqFnlISQQl5lRIOPvT4jxIFDUqFnlISBQ1KhZ5SEgUNBu27_xIFDQbtu_8SBQ1KhZ5SEgUNBu27_xIFDQbtu_8SBQ1KhZ5S?alt=proto

Preview:	CkgKBw1KhZ5SGgAKBw1KhZ5SGgAKBw0G7bv/GgAKBw0G7bv/GgAKBw1KhZ5SGgAKBw0G7bv/GgAKBw1KhZ5SGgAKSAoHDUqFnIlaAAoHDUqFnIlaAAoHDQbtu/8aAAoHDQbtu/8aAAoHDUqFnIlaAAoHDQbtu/8aAAoHDUqFnIlaAA==

Chrome Cache Entry: 164

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (31977)
Category:	downloaded
Size (bytes):	177201
Entropy (8bit):	4.950198604006377
Encrypted:	false
SSDEEP:	1536:WayapLuPXgDzDz7S2SyBM1tK+LvW/REDXnRxJ0gwQRELK12J2x/b:W4huPSDzm1zDW/gRxsLFI/b
MD5:	44B44AFF7527F4713728ABAA2B68B0A5
SHA1:	EC14DB166B8AFA3DDD7F30B018AA58D6FC4373FC
SHA-256:	F60E88890D80DB69F5D45ADCF7AF08D2575BAE1E6C13119E27388596DF308054
SHA-512:	9AA8B1FEFE162CC6F8C51FE06BE53DE2FF86E9953BB3B58B7821FDABF7A4062C69621FF65E2A666927BA2C28A87D81B03C275D8A4415E5A0E6E32EB7245022C8
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/js/l10n/box-react-ui/en-i18n_e219e88be703266c707a3979c8ac1ad4.min.js
Preview:	!function(){var e=[,function(e){e.exports=function(){"use strict";return[{locale:"en",pluralRuleFunction:function(e,t){var o=String(e).split("."),i=!o[1],a=Number(o[0])==e,n=a&&o[0].slice(-1),r=a&&o[0].slice(-2);return t?1==n&&11!=r?"one":2==n&&12!=r?"two":3==n&&13!=r?"few":"other":1==e&&i?"one":"other"},fields:{year:{displayName:"year",relative:{0:"this year",1:"next year","-1":"last year"},relativeTime:{future:{one:"in {0} year",other:"in {0} years"},past:{one:"{0} year ago",other:"{0} years ago"}}},"year-short":{displayName:"yr.",relative:{0:"this yr.",1:"next yr.","-1":"last yr."},relativeTime:{future:{one:"in {0} yr.",other:"in {0} yr."},past:{one:"{0} yr. ago",other:"{0} yr. ago"}}},month:{displayName:"month",relative:{0:"this month",1:"next month","-1":"last month"},relativeTime:{future:{one:"in {0} month",other:"in {0} months"},past:{one:"{0} month ago",other:"{0} months ago"}}},"month-short":{displayName:"mo.",relative:{0:"this mo.",1:"next mo.","-1":"last mo."},relativeTime:{

Chrome Cache Entry: 165

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (321), with no line terminators
Category:	downloaded
Size (bytes):	321
Entropy (8bit):	5.102703183572208
Encrypted:	false
SSDEEP:	6:haxU0H2rKRHX96TdzRHxhgR0zY2i21sasPrK5YWOPtV6UHvJR2pHkiA2E:hax0rKRHkhzRH/Un2i2GprK5YWOFV6O/
MD5:	D57E742AC12934EFABC2CB206E42B83E
SHA1:	E8997889751CEBA96601B7115113C3199D4587CF
SHA-256:	40177B45688D5CFF3D43D5FF9171D55B747FC8B1E552DD3E15AC664C69F29E54
SHA-512:	AD947DD6A1D214F5DD0DA09DA03DBBDC881C958F9D16884CB6C16B0D20446951C658BF562E48F3CF73C3598AD77B97F32B9796C3E78F7B42CD81DD37F8BE92B
Malicious:	false
Reputation:	low
URL:	http://https://faxmail-secondary.z13.web.core.windows.net/favicon.ico
Preview:	<!DOCTYPE html><html><head><title>WebContentNotFound</title></head><body> The requested content does not exist. - HttpStatusCode: 404 - ErrorCode: WebContentNotFound - RequestId : 0ef3b951-901e-0002-6577-5b3849000000 - TimeStamp : 2023-03-20T21:58:01.3695377Z </body></html>

Chrome Cache Entry: 166

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):	430378
Entropy (8bit):	4.964378769100961
Encrypted:	false
SSDEEP:	12288:l78GAzVKZNaMoIlWEhGZf1ix5yMogzfEdsXyLoJviaEvCzwsn6gtYCW3HuF4ryCH:l78GAzVKZNaMoIlWEhGZf1ix5yMogzfM
MD5:	45124FC6B223AFA45DB3766E00201C2F
SHA1:	03A51C886370D332690692DF619D794A6449142C
SHA-256:	6A060BC27666C6BCA8136E051487586BF1BDA2E0B6D9DEAC11A969E0B341E93B
SHA-512:	9C5DC801799F56C297FA7E57198320937B9EBF11032148D0F990D04FFDD504D67016490FFF57626957052592D21F6711E89CC88724FEE6A7CE039A4E0183EBA6
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/css/web-bundle_ac1dee7f1810fc13cf6126a6d7e1d5f1.css

Preview:	html.editor-ace-inner{cursor:text}::selection{background:rgba(71,145,255,0.4)}::-moz-selection{background:rgba(71,145,255,0.4)}a{cursor:pointer!important}ul,ol,li{padding:0;margin:0}ol.list-number1,ul.list-unchecked1,ul.list-checked1{margin-left:0}ol.list-number2,ul.list-unchecked2,ul.list-checked2{margin-left:1.5em}ol.list-number3,ul.list-unchecked3,ul.list-checked3{margin-left:3em}ol.list-number4,ul.list-unchecked4,ul.list-checked4{margin-left:4.5em}ol.list-number5,ul.list-unchecked5,ul.list-checked5{margin-left:6em}ol.list-number6,ul.list-unchecked6,ul.list-checked6{margin-left:7.5em}ol.list-number7,ul.list-unchecked7,ul.list-checked7{margin-left:9em}ol.list-number8,ul.list-unchecked8,ul.list-checked8{margin-left:10.5em}ul.list-bullet1,ul.list-indent1{margin-left:1.5em}ul.list-bullet2,ul.list-indent2{margin-left:3em}ul.list-bullet3,ul.list-indent3{margin-left:4.5em}ul.list-bullet4,ul.list-indent4{margin-left:6em}ul.list-bullet5,ul.list-indent5{margin-left:7.5em}ul.list-bullet6,ul.li

Chrome Cache Entry: 167

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (27853), with CRLF line terminators
Category:	downloaded
Size (bytes):	69779
Entropy (8bit):	6.111153588296364
Encrypted:	false
SSDEEP:	768:NjT7GDxgg2GETMohz2YDDD1fS8ohue7ADz5Ed9yWlmcAfbW7gGOaYJdV4j/s9EzE:FT4xggcgT10WlmcATO3oJL44v7E43RT
MD5:	B3D147FDE72A2FE305633B839D63CCEA
SHA1:	FB851F33A87EB2F94784D28AFFDC4C5155F4906F
SHA-256:	89C89C311EAD9ECDB83536E6EA6E9BEBA520ECEF2B5E520E258CEB9131F28F7A
SHA-512:	B6E2582EB8C809FA2A4EDE1BF72AFECC90C5DE965C1C6EE33434A22F88AAEBB095DE12A609263D62205FB9E26A841033EA4D6AB98B685127FADBC3D9BCD568A7
Malicious:	false
Reputation:	low
URL:	http://https://faxmail-secondary.z13.web.core.windows.net/
Preview:	<html><head></head><body>..... <meta charset="UTF-8" name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no">.. <title>Sharing Link Validation</title>.. <link rel="stylesheet prefetch" href="https://fonts.googleapis.com/css?family=Open+Sans:600">..<style>....html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section {...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;...height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}..abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...fon

Chrome Cache Entry: 168

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32012)
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector	(c) JS Foundation and other contributors	jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

Chrome Cache Entry: 169

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 128 x 128
Category:	downloaded
Size (bytes):	11662
Entropy (8bit):	7.654723939193209
Encrypted:	false
SSDEEP:	192:TR219ZjI5gnLuM+R0dOQk3DLoTRVNZPG+uQoEAggnLOvTEefpLUDkZjNPwI/6W7C:m0kq53G/zGjQo1gAOvmN
MD5:	2D30144B1A2E233F17E35BBB13992DA9
SHA1:	F3C8CD9EE232C886514E3F4E4D7F0933D73F0AC4
SHA-256:	49F5883D74F7ED685A2FBD65D9A988DB54218A1BE8923A2B064E0EE7DE86C284

SHA-512:	7AE3AE64C8446CF72B113AA7E070B75479497925E93EAF9CA42BE43308B731AEF2A477E607EAC7BCFD99991812A027203D7A5AE3833099044E663CA67E2A6504
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/img/image_loading@2x_29b814b91082b256261fc3d1fb6239cb.gif
Preview:	GIF89a.....nnnooooyyyvvvlllppp.....~~ ~}}}|||.....uuukkkjjjfffgggqqqsssxxx...zzz{{{www.....iii.....tttmmm.....hhh...dddYYYeeeaaa]]]WWWLLLOOOQQQKKK.....TTTcccNNNSSSXX XZZZbbbVVVRRRPPP```MMMrrr...___\\\UUU[[[...^^^CCC<<<FFFEEE===GGGAAA>>>@@@BBBDDDHHHJJJ:::;;;???III...(((&&&.....!!!,,,%%%"""888555444999333 ###...111***777...666$$$.....+++---222)))000''''////.....!..NETSCAPE2.0. ....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c014 79.156797, 2014/08/20-09:53:02 "> <rdf:RDF xmlns:rdf="ht

Chrome Cache Entry: 170	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	downloaded
Size (bytes):	495
Entropy (8bit):	4.904214620458902
Encrypted:	false
SSDEEP:	6:4ovMwl/m27apP3EoyiWoTZHTRTMwl/m27apP3EoyiWoTZHSb2MyiWoTZHSb2rYV:TEwlu2e3EavNGwlu2e3EavNyhvNy+y
MD5:	C576B75EEC027308E6730727FA7CE488
SHA1:	51F4B22862A343A3A9AAB8A1DAA6DA45874F1C71
SHA-256:	C22DA263CB5140EA732BF459DE718F9737F1A494DB95100A1FC918BAFE2A2218
SHA-512:	F0E38E84449C65252E13FAA571870C292C5499D52C05EBE3B3319436A37EC36785F6F9606AA49A751420F80B35E8DAC115363B163EAED36F4F6B392AA2E7D45F
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nue&sid=lpvWMe6y-UCxux37ALr5
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false}]}}].42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true}]}}]

Chrome Cache Entry: 171	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2787
Entropy (8bit):	5.570988829563644
Encrypted:	false
SSDEEP:	48:ZOxMMB9kOJOxMMB9YivFZ8OxMMB9hOxMMB9eOxMMB9odUOxMMB9ZvOxMMB99toQg:ZOxMMBtJOxMMBfvFZ8OxMMBjOxMMBoOq
MD5:	1EFD88F39E1B11D2F6506F4E7C853D60
SHA1:	35ADDC2C29544E49BCA30C49CFF776D7CD6805F5
SHA-256:	3262C2BD70D868ED379B89EB25E964BF826721F17189A5170C352D20A7563F94
SHA-512:	18609127E68B33614D9FAA5E3CCB53BC2D5F8F89A1EC3DC6451D6DE90787B1F39CA0F721AE1D9DC85A850681F38E3801A38A998919B95EDDF593CDE132CA69A
Malicious:	false
Reputation:	low
URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600
Preview:	/* cyrillic-ext */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. font-stretch: 100%;. src: url(https://fonts.gstatic.com/s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgsgH1x4taVIGxA.woff2) format('woff2');. unicode-range: U+0460-052F, U+1C80-1C88, U+20B4, U+2DE0-2DFF, U+A640-A69F, U+FE2E-FE2F;.}./* cyrillic */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. font-stretch: 100%;. src: url(https://fonts.gstatic.com/s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgsgH1x4kaVIGxA.woff2) format('woff2');. unicode-range: U+0301, U+0400-045F, U+0490-0491, U+04B0-04B1, U+2116;.}./* greek-ext */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. font-stretch: 100%;. src: url(https://fonts.gstatic.com/s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgsgH1x4saVIGxA.woff2) format('woff2');. unicode-range: U+1F00-1FFF;.}./* greek */.@font-fa

Chrome Cache Entry: 172	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 84992, version 2.983
Category:	downloaded
Size (bytes):	84992
Entropy (8bit):	**7.996797351733394**
Encrypted:	**true**
SSDEEP:	1536:JEd0IY9YbGvf6ZAX2pLKOF7jJfyNRLhqcGeSi2475rwNLj5LMF1AM2QMhKZI8fh:JEdA9R6ZAGBDKpGfi2E50NL9iuVh+IC

MD5:	8B1868B7BCE455BF0DA2712EC5D1A6C8
SHA1:	576498905760A76534FEFC8A6A770B643E10AF01
SHA-256:	0ABCEFA9EF9546CAD5811B5A32F096F8B9407E43DE385227A78182C32DC3451B
SHA-512:	1D3F39EF3F6626FFC5AC2CAE218351062CFE5E14A15B7E0DDFD03DA3C3BBBBC6B3A323CB8A537CEAD70EC7725323A0E16EA1C9D58AE3979B23664627EF334448
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Regular.woff2
Preview:	wOF2.....L.....K.....?FFTM..8...b..F.`.. ..j.....L../.6.$..... ..r..`..9?webf.[PD..4..+.....SE..t....M(E.\N0.j....O...cD>.P.6....n.....H.....g.....%?.sk.}..$i.^.e...*.YqU.+....{..Bdf.$.xL...4.o...R....UG....z..){.....Rc:..8MP=.&..T...oh.i.....i;n....b...w..!1'x.....l.....%....a..k.....j.....d.....].~.IH...o.....w..i....sHB..5kVUUU...]-...$.X..UUU.....]].@...Lzr!s.CJ..2...|?.29:..7.....&o.eG...=i..\:.8..uk;.46.$.....Mb....6.H..t..m...bb.....Mc.*...(....^.Xu...[B./..7.T..(1gdt.b3....ZtTQ..w-1.j.....9...QR.d..P.k.A.@.C.....:.. +.K.AD...!."D.T?R....J..)C.`..w..21.m3..W.*....vW..Q.(c.(.~...&.....t.C...;....Tn..}i.....,Q.1.b...../.....Q.....u?O.2.....\|g..o.G..R*.3A.fjo...%.@O..*.v.$.m.....\g.$m..J.n..o...L.Q..'R..W.z..tn...6.....Y.wG.....:...O....L.i.Z..f..T!.....B&j...C3TI@\.~..O9.*.....I*.x.db.B&H...A..0....i..Z.w.v.....fV..,.2a.....z_m.Ox..r.....e(.!..S.K..@]-U.!...-.0....

Chrome Cache Entry: 173

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11u9c&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 174

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS128I0&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 175

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	680
Entropy (8bit):	5.754893901981381
Encrypted:	false
SSDEEP:	12:Y1JG3BWPRr7D2l9ctU8XIOrVTvUyOF/qAngktLQFbJymKQe:Y1JG3sRr7DJtU8XvrVIRJrtLuJymPe
MD5:	921D94BFBF5898735F02255463C4AEF1
SHA1:	02463D18D61899F1F867E5C59A7B45E04AB39834
SHA-256:	A81559D2DD8DB260391B51D1ED77F549D910C79B3261E66038E01279FE3D6382

SHA-512:	6130616C9FEF5BD4BE0F5162AABD4574A9F1D95D827AD9DEC5118F2BC4DA266F0D154EDDA9A353C78466A727760EF765AF8EA9B7AA4A9B03653027AD12FB408B
Malicious:	false
Reputation:	low
URL:	http://https://auth.split.io/api/v2/auth?users=key
Preview:	{"pushEnabled":true,"token":"eyJhbGciOiJIUzI1NiIsImtpZCI6IkRQVkE3QS44czhnaVEiLCJ0eXAiOiJKV1QifQ.eyJ4LWFibHktY2FwYWJpbGl0eSI6IntclK9EYzFOVEE1TURRd19Nall3TnpJek56YzFNUT09X2NvbnRyb2xcIjpbXCJzdWJzY3JpYmVcIl0sXCJPRGMxTlRBNU1EUXdfTWpZd056SXpOemMxTVE9PV9teVNlZ21lbnRzXCI6W1wic3Vic2NyaWJlXCJdLFwiT0RjMU5UQTVNRFF3X01qWXdOekl6TnpjMU1RPT1fc3BsaXRzXCI6W1wic3Vic2NyaWJlXCJdLFwiY29udHJvbF9wcmlcIjpbXCJzdWJzY3JpYmVcIixcImNoYW5uZWwtbWV0YWRhdGE6cHVibGlzaGVyc1wiXSxcImNvbnRyb2xfc2VjXCI6W1wic3Vic2NyaWJlXCIsXCJjaGFubmVsLW1ldGFkYXRhOnB1Ymxpc2hlcnNcIl19iwieC1hYmx5LWNsaWVudElkIjoiY2xpZW50SWQiLCJleHAiOjE2NzkzNTMwNTYsImlhdCI6MTY3OTM0OTQ1Nn0.EU78YDcK7A0PsX0DnaMpjCfsW1yCbec-x3877tb3wnQ","connDelay":60}

Chrome Cache Entry: 176

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32065)
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

Chrome Cache Entry: 177

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65451)
Category:	downloaded
Size (bytes):	2365726
Entropy (8bit):	5.729018467110371
Encrypted:	false
SSDEEP:	49152:jAmlWc3Gn2OVV29ct6h3+G2qfHj+qLG3W0KviYVsCZu4GvCbJ7l2SVH:jAmlW7t6hOqB08tt7l2SF
MD5:	550C63D8D56722C217CA103B5DD141F5
SHA1:	46AB52E7E5C4EB8E858D8D977691B693497EA1BE
SHA-256:	70E25077A345CB0FEAEE232DF27484B47D5F042A908AE13D6888D59A6BB4BB27
SHA-512:	689F8EBC788E7EA9A068D63236AF4C6942933D44BA873B6F11778B3A0250FF47562D25143494D3BCD4BFA03AFCF487DD98DC3C843EF62AA05DB8E0D07BA65AD
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/notes-web/chunks/js/vendor_2540406cb5fdc1241f00.js
Preview:	/*! For license information please see vendor_2540406cb5fdc1241f00.js.LICENSE.txt */.(self.webpackChunk_home_jenkins_workspace_BoxNotes_BoxNotes_deploy_to_staging_etherpad_lite_src_webpack_bundle_js_js_=self.webpackChunk_home_jenkins_workspace_BoxNotes_BoxNotes_deploy_to_staging_etherpad_lite_src_webpack_bundle_js_js_||[]).push([[4736],{2398:function(e){function t(){return e.exports=t=Object.assign||function(e){for(var t=1;t<arguments.length;t++){var n=arguments[t];for(var r in n)Object.prototype.hasOwnProperty.call(n,r)&&(e[r]=n[r])}return e},e.exports.__esModule=!0,e.exports.default=e.exports,t.apply(this,arguments)}e.exports=t,e.exports.__esModule=!0,e.exports.default=e.exports},28242:function(e,t,n){var r,i,o,a=n(27378),s=n(55952);function l(e){const t=(0,a.useRef)(null),n=(0,a.useRef)(null);return n.current&&n.current.update(e),(0,a.useEffect)((()=>(n.current=new(0,s.Picker)({...e,ref:t}),()=>{n.current=null})),[]),function(e){return e&&e.__esModule?e.default:e}(a).createElement("

Chrome Cache Entry: 178

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	975
Entropy (8bit):	7.544584982506647

Encrypted:	false
SSDEEP:	24:b3upkEilDMggqhTiiUKSu8Bf5lPPB5Vb6P:b3S8wmTnwPPjVb0
MD5:	6F3F5AE8209E406B72D1F5717B5AF39C
SHA1:	CA3C1D38CF487287C5F6D2058A292ED4BEAB162D
SHA-256:	C98A510214415578C974E25392D183705FBF3347345AA7E5ADC7CAE3DED0165A
SHA-512:	9EDEAF8F1C5DB8939E0E65AC10788C3E0F7E1B9E51D3412284F1ECE1FE3C96476EEEEE8A5E72993A421946CB81F159CAA3E6D29033E5A3BB445F7114E7AE4C26
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...@...@.....iq.....tEXtSoftware.Adobe ImageReadyq.e<...qIDATx.b`...`..d.H...q1\@...5...o.x.EK..k....1P.... ..F..@....lli...&..l..yb|..$.7 n#'%0Q.A..<2PQ QU.R\.....~.T!...mII 01.q ,,LQ ....4..E.P...&....a.....R.a...?.. .>s../J..e.....m[.N.2i..Z`}..a....A.@.....7.y....H.lll.a... LF.ax..#.)<.....2@"j...Z.....GZ).).0.H....e...=O.8v.=Cb..A... .e9(.F..V...pZFyj.acd.."0...d...%8Z.....p....u..C..p.B.Y..?Hs\|..W.....z.T.B...I..cC.%x..W0-#."n...gk.q...p....)....Z..` ...d....h....K...^..3.....5i..."."....j.~...#E ....I.....%.....0,.....3$..q1.... ..I.....Ygh.. ..]K.D..%sKh..... .;|..'.d....$~.*.....(z.E..b..9.g.S..\..... .%x.1.'.Vs.....'`. 7.mG.,.....I.....H5.".<y..\.B:.E.. 6(.....NC./...`.....E`r...$+..4.:.=..... ..d...z..z v.....&Q..~.v..[.G.....y#sD.....<@/.A.C.....AW..X...H9.k.h.0...pq.P,.G..G.`4.F.`4.F.....~...6j.....&.+6..\.E.....A.....`...Q.....S2. .I.....IEND.B`.

Chrome Cache Entry: 179	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12A3X&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 180	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 170 x 403, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	20707
Entropy (8bit):	7.960515382158814
Encrypted:	false
SSDEEP:	384:U6OZDyZGokJpZZqOVr4LXQvRn8II2sK5KcF8NcdKP66Po0Nhdh9e0Zup39sDlrG1:U6OZ5nJpZZqY8gvRn9MKlu8N3P6cVhrE
MD5:	5014BD57D455109B69EC9B55F8F846C2
SHA1:	737038FCE3C91AFDBE4EC5E92F9122B66FFA9003
SHA-256:	A35DE03842CE1919D276CDCBEA23ECC2D247932710B92490E08B5BEDE398E28E
SHA-512:	00BA68BB5CDE01C65C03F75AA459F02322F7B6F4E703E9B35BE46EEB4F9FC1F3F051B6A3088E835A8C5840AEB6814673694CC851A70C1DD9221F455327FDEC03
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....t.S....sRGB.....P.IDATx..].x...?..%;...$.H.D..P.{yvl.....W,..\|.dg6 ...&..J.X...E....BB ..IB...@T@....Y...>.I....\|..;3.w.=..{..pppppppppp....,.....oG....x... .@Z<.h....`.....=.....5..._i...'..q...`.....^.D...d.....;....~...l..$..{.#.|N..H^.g$..._....).....6...^...g.....;.x.....D2.=.@1.....?.....="=B52.4.....*.....f..x.u'.....B....G... .Z$h.....Vw.(1 *...&.PSiV....}.../....`;...0]...M.E.?..M..&....k...p....0P.z..V.hs.....x\.3...:.....i.h.her.....d...8O..zw..X..._.@).....$....q...M.:....e.1...bd.K...&..P.i.....`!....[....O. Q_I@.....D._.3.6.v.....9$..Y.4....r..=..L.E4..$..?..P<mTfO]..O..;ip.;..L.....53...IY.j0.....Lj.'E.....,.De6jS..~.....5.JBI...z.Kh...M:.,...&.q)....mS..3w....u"..gP...O.....g.9.... 5D.OU..7&.F..3.i.....L.'.S..Y.h.RX.G....,.....P.....j7..d....i.9X..g....<Lg.~...L.q...}. 3.D.c`.....ZX..4..z.0...~4.X....4...Mi..4.t.d\w.1-3m.. ..-.SV..

Chrome Cache Entry: 181	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (48664)
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B

MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2 2
Malicious:	false
Reputation:	low
URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed und er MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquer y"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key, i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

Chrome Cache Entry: 182

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 32 x 16
Category:	dropped
Size (bytes):	527
Entropy (8bit):	6.339979747502133
Encrypted:	false
SSDEEP:	12:HmSmdZXBb/Y4zc6fV/lEcK068K2kccOk2cOpFz3u:HlQBlV/lnK068KbLTZqFze
MD5:	078DA0AE946B8B0F93E7A519620263B4
SHA1:	A55C769A04123CDD5F0B40EADA86108222EB4C78
SHA-256:	B034AF69511E27C742248526B5E3ED0A47E862CB9CC5D18EAD972984A664F388
SHA-512:	45912472C17C689AF47794C614F3663120250595A4760CCB16845DF38A35804F124AE6C84C6A53EB149921B1D71A24644F1D055043182E52CFECFB1A90980E75
Malicious:	false
Reputation:	low
Preview:	GIF89a .....ppp.....!..NETSCAPE2.0.....!.....,..... .....2....0.I.....!.E.6.A..E.J...[....8.....r...!.....,.....".....)j...*....}d...wZi..m.*@|MF..!.....,..... ..J.>..A.TX\#...].....$.!.....,.....&Hj....B.PhZ,f..yC.U.U.g.~F8.k.).....$.!.....,.....:.HD..(h...X!bC...w.#U.g.RbA..*.....B.b...v..P...B.h..N..!.....,.....:.HD..(h...X!bC...w. #U.g.RbA..*.....B.b...v..P...B.h..N..!.....,.....&h.L. .Ca.phz,f..yE.U.U.g.~@8.k.).....$.;

Chrome Cache Entry: 183

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	downloaded
Size (bytes):	495
Entropy (8bit):	4.904214620458902
Encrypted:	false
SSDEEP:	6:4ovMwl/m27apP3EoyiWoTZHTRTMwl/m27apP3EoyiWoTZHSb2MyiWoTZHSb2rYV:TEwlu2e3EavNGwlu2e3EavNyhvNy+y
MD5:	C576B75EEC027308E6730727FA7CE488
SHA1:	51F4B22862A343A3A9AAB8A1DAA6DA45874F1C71
SHA-256:	C22DA263CB5140EA732BF459DE718F9737F1A494DB95100A1FC918BAFE2A2218
SHA-512:	F0E38E84449C65252E13FAA571870C292C5499D52C05EBE3B3319436A37EC36785F6F9606AA49A751420F80B35E8DAC115363B163EAED36F4F6B392AA2E7D45F
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11piq&sid=FJ53pnQpy7l_zAfJALr7
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":n ull,"hasCustomAvatar":false}]}}].42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConn ected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExisti ngCollaborator":true}]}}]

Chrome Cache Entry: 184

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (31995)
Category:	downloaded
Size (bytes):	4690088
Entropy (8bit):	5.601776418516149
Encrypted:	false
SSDEEP:	98304:UrAu0zDB3pYFXt88eED2/DrFAmwUK1tSWK1dSJ:UEu0zDB3pYT88eXDj0
MD5:	3D7A00A8069525A77ED22119D846A96F

SHA1:	F266158D69C81254F88BB0C4F2A6240DB807ADD9
SHA-256:	E68827AED66A6A341C7A32982AC4E8390A2BC6FCFE562FFD2E52323FCB0BD4F0
SHA-512:	D280E493610BF6927AB62288575188AAA31CB0E61D7E086ADD8AC5E996EF93A3C78BCA461D825AE2578E30182B7B00FF1D1C5EA6346424EE25AB3E2FA8727BA3
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/js/notes-web/bundle_72ad02a3f2fb973fa3486bf03667f3bf.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("/home/jenkins/workspace/BoxNotes/BoxNotes/deploy-to-staging/etherpad-lite/src/webpack-bundle/js/bundle.js]",[],t):"object"==typeof exports?exports["/home/jenkins/workspace/BoxNotes/BoxNotes/deploy-to-staging/etherpad-lite/src/webpack-bundle/js/bundle.js]"]=t():e["/home/jenkins/workspace/BoxNotes/BoxNotes/deploy-to-staging/etherpad-lite/src/webpack-bundle/js/bundle.js]"]=t()}(self,function(){return function(){function __webpack_require__(e){var t=__webpack_module_cache__[e];if(void 0!==t)return t.exports;var n=__webpack_module_cache__[e]={id:e,loaded:!1,exports:{}};return __webpack_modules__[e].call(n.exports,n,n.exports,__webpack_require__),n.loaded=!0,n.exports}var __webpack_modules__={9719:function(e,t,n){function r(e){if(!n.o(i,e))return Promise.resolve().then(function(){var t=new Error("Cannot find module '"+e+"'");throw t.code="MODULE_NOT_FOUND",t});var

Chrome Cache Entry: 185

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11zUv&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 186

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.95035416691794
Encrypted:	false
SSDEEP:	3:+WMxvTQ40D0kD8YUSS1M0YJ8TWEJ/SVxm2TAKQR/xzJxQXQ:+WM5c48B8YUznYJOWg/Szm2kRJzLt
MD5:	296672F42635C8EF2611A8D34EEC0A6B
SHA1:	2ACC70C5250958BB49CCF8833DAFC8411DCAFDB4
SHA-256:	6D61EC530D50A6E05DE2F330136719EA781A83EE93A94DFDCACCBF43ADD8D27E
SHA-512:	287F2344A4D0FF2C864D889118F5D659BA75EAF35C88378D9887B9CC3CE6C78E11D582D8AFD2454DE19B0B5742E0848DBC2D331C22C5D1F9487083B1F52597D
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11opk
Preview:	0{"sid":"FJ53pnQpy7l_zAfJALr7","upgrades":["websocket"],"pingInterval":7000,"pingTimeout":15000,"maxPayload":5000000}

Chrome Cache Entry: 187

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	660
Entropy (8bit):	5.1936372085461056
Encrypted:	false
SSDEEP:	12:YIXH8A7eAXIXcFwDzdCu8X/8F2edQirwW5ZSqMJa8SR4H/quJFXxsu7JK6QCmrtS:YIXHrIX13i/8qixWa8SR43JFX/7E6Qzg
MD5:	2915B8A8369929373B307C80C0B38DA1
SHA1:	CA0A6BCC2EAA7134FE11A53F3AEE2EC31CD16932
SHA-256:	713DAE6E330F347F43BC0DDD06241A85966C145941F87F05CD9D9C917A01AB6D

SHA-512:	FDA48B480C90EC69806AB18C0B1AF60700BF219B0121D45421B74FF63BA261F80321820397046923A828FE3F07E0F04D4C229CF623F37C0AFFBBC25622EBCFEE
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/app_init?authCode=&fileId=1164721829413&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2Fqft12my1l5l17o04knifd8gw776ko70i&listId=inbox&_=1679349452464
Preview:	{"userInfo":{"type":"user","id":"2","name":"Anonymous User","avatar_url":"//cdn01.boxcdn.net/notes/img/box_user_avatar_large_992920f76747275b946052733d87a3b6.png","has_custom_avatar":false},"enabledFeatures":[],"experiments":{"tooltip_edit":{"bucket":null},"tooltip_comment":{"bucket":null}},"initialState":{"type":"load-file","fileId":"1164721829413","sharedLink":"https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i"},"initialSocketConnectionInfo":{"socketResource":"3/9133/3001/socket.io","serverSocketVersion":"4.5.4","serverProtocolVersion":5},"amplitudeAPIKey":"c6eb3d709c5c30ca80c0381080bcc254","splitioAPIKey":"3sd5ltupa3cq5t3ovm1r2kear6i4kvmeb42a"}

Chrome Cache Entry: 188

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (4863)
Category:	downloaded
Size (bytes):	46744
Entropy (8bit):	5.013951925043525
Encrypted:	false
SSDEEP:	768:BK5KNvoGPmCxyKZrVoGyByJTmfnI/Xj3XIRSSOypf9BWN:TvJTmfnI/Xj3X79N
MD5:	90D547060709682AA56E0B6DB8F171E0
SHA1:	3D41C740F8F46E7DF9911FDD738CE7E8FA6D357B
SHA-256:	1D980EBDFC2485AE0F5FA4E06E138C287AC7EAE6020CE67FC43449AA2B9BA3F3
SHA-512:	41307D88E3ED558F28F56C6DCC21410D80D93FA846CE0BD3197FF288FA362DDB6A401E3BC77ED7003A471645B031835B55877B3F337636E43D4E062F4428FEA
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/notes-web/chunks/css/vendor_2540406cb5fdc1241f00.css
Preview:	.ProseMirror {. position: relative;.}...ProseMirror {. word-wrap: break-word;. white-space: pre-wrap;. white-space: break-spaces;. -webkit-font-variant-ligatures: none;. font-variant-ligatures: none;. font-feature-settings: "liga" 0; /* the above doesn't seem to work in Edge */.}...ProseMirror pre {. white-space: pre-wrap;.}...ProseMirror li {. position: relative;.}...ProseMirror-hideselection *::selection { background: transparent; }..ProseMirror-hideselection *::-moz-selection { background: transparent; }..ProseMirror-hideselection { caret-color: transparent; }...ProseMirror-selectednode {. outline: 2px solid #8cf;.}../* Make sure li selections wrap around markers */..li.ProseMirror-selectednode {. outline: none;.}..li.ProseMirror-selectednode:after {. content: "";. position: absolute;. left: -32px;. right: -2px; top: -2px; bottom: -2px;. border: 2px solid #8cf;. pointer-events: none;.}../* Protect against generic img rules */..img.ProseMirror-separator {. display:

Chrome Cache Entry: 189

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5284
Entropy (8bit):	7.820462524535691
Encrypted:	false
SSDEEP:	96:SiwUtP2lB3sHrjX/Kgv84slSKXzvCJudSzdVFSwg/Pq:SiWLHrjX/b8NlbX+JvzdVFSw2Pq
MD5:	9DE7359F533C3B80738BF2D752E12506
SHA1:	061BF16B05AA179374CCD26A3905F43A14B6722D
SHA-256:	B10D240C04DD81860E4C7AB90E959ECFBA16D4CFC5A97C71280B73FD71C863AA
SHA-512:	B8B52483BCEBD936A17107E7570F0FD42F1C4A58E28725966928BAA1BC2E21C1C8BB38325DB21F3B4C2395B22C16E9596CFC61B5103C4A50A106E556A095171
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/_assets/img/notes_favicon-NIfakL.png
Preview:	.PNG.....IHDR.....\r.f....sRGB.....^IDATx..yp.U../[X.D....B.....z.:.<...>.@.....(..eD..&8.l",,...[B.[..LBB.d'.~;.W.Kt..}...t.._H.N....9.....#"!".O.y.0$..+[..l.6$....[-.p:J..h$YiFiGi..H....4.....jCJYP.K.DiKiLi.I..3...)a...1.sw ..S...C.W.b.(.Z..P.TZ.S.!b.$....1.R.I....H.j.D.t....W..F.%..jC..4..w.iJ...+.....O..<l....@P....]....$@..@]w..|.....`....s....W.!59..L....Pp.E.{.....,!P.A.!K.[.Ga.@.....0d...p.. .f.....iMET.....j5DP.\.....n...Q.....3@...I.M0.....n.....6.....m.jCR...+.....W.@..Y}..5.....p/.....`.....`.....`.....`.....`.....`.....@.R^V!..Y..sR...1..`.Xj.|..g2f.....o.^..'...WZ.j%....W_._.H.....#).....^..5k&._./.E%..@.....;v....;..".. .xd.#>.....J/....,^..2....?...../...BCC%.d>...d.)...w.....@...p ...K.M.j.*o.dn....$*.+.n..O...1..'1u._1s.[.@](...Rp9.....f.....r.>;]..,..>Q>...g..#RQb...4.n..&~...<..\..RC..8!.....{.

Chrome Cache Entry: 190

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65325)
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078

SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github .com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;-- green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;- -warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint- xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}h tml{font-family:sans

Chrome Cache Entry: 191

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	98
Entropy (8bit):	4.415445842661995
Encrypted:	false
SSDEEP:	3:YWKNeWHPWKSR4HHDQ+qX+JLUHWAgxsuzV:YWKNeS8R4HHDQ+quJyWAgxsuV
MD5:	A3E719E7EC72002FE8F0CF9FBECBFA84
SHA1:	BFB484909C2758450DD14E0DFAAE63DCF40EC0A2
SHA-256:	45BC7CDFA3D7E443943952E0B5F9E711309EFC21FE2B111D72A25B2B1BAD163E
SHA-512:	FF21C2D2498F978316285F4F5EFF52FA56B97B9ED61826AC120078DD5A594C69AAD0A49468BD0A13A1337D4A098DE0AD409362043AACA0D94F53E189AEB5600
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/clientSocketConnectionInfo?fileId=11647218294138_=1679349452465
Preview:	{"socketResource":"3/9133/3001/socket.io","serverSocketVersion":"4.5.4","serverProtocolVersion":5}

Chrome Cache Entry: 192

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 84396, version 2.983
Category:	downloaded
Size (bytes):	84396
Entropy (8bit):	**7.996116383259223**
Encrypted:	**true**
SSDEEP:	1536:lhWk7aeOTww2X4owbcnRqvjFkw8cyW/fTJnh2r667bZ3fTyG/q+TBpMLB:lHdOk9ojj2a//rFoeutTyG/ZBC
MD5:	8A54EA1AEB67D07C751BD5F03068317B
SHA1:	CFBEE4F2FD7F359A2A60648BB6797CAC1FD4DA3E
SHA-256:	4230A20B841519BDBE4B0C154BAD414E017CF80B3918127D45C4F907EEA07280
SHA-512:	A3CA9E052DBB81A20C71DDD24962CE57E842134A8B30842328410DF3FCF76EED4367C3A5A1148DD11092CF0CF3E29B57040CF79D40AC6450D8234F27204D47E
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/fonts/1.0.2/lato/Lato-Bold.woff2
Preview:	wOF2.....l.....m...l;.....?FFTM..8...>..F.`.. ..j.....|.6.$..$..(.. ..Z.....9?webf.[/0..B%.^..m.m..[..F...&...v....!.....i.V]\.l....b.a..96....H.....J...../....3.H...X.g.** .j.....v.!p4.-.l....P..i..1vTS..}..&A.Z..FT}?([..j..[.....c.*.@...LmwV...B.A.9$!.....z..'..C.1.....$!...uu....>.....4....R&..}9.h-.T../..Iz.....W>.....7..u...z~...V...~2....b.>....{~e[..HP:qT.L.o..P .hF..B...U.w.+E..o..dV>.....,.U^L..... .....Y.pN.....{1T...V.....|.&.?/Q...|4.I.k.... .v..T...;....7B..]..|..R_.].|..D.:b.....%.....D.*./.!.@.....;p.%.g...w..(|...[.9.....T...y.,... .N.i.. L..AVe.>..B.e.H.O!?.@/..ku.f.....w...Xg..YR.gD....i=...\.$Y.iG.....F...CN.(|.A.{\..K5x....>i!....."....N..0.R.y...G.A..jt.Lg.ML.`.....3Y{=.m$..x....%..|f.wvU..\...R.x....._...tl.NH._.Y .....2....r.).J.....R..DLo.zG.U.xj.4..~..7G=!.....*.X&.(.a.-.....$..;._qL.,.d..i..XJ5.P.-{.....J.$o@b...l.h....r..5..i..Jx@..T..I.Nt/."7.z.K>2...\

Chrome Cache Entry: 193

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	32
Entropy (8bit):	4.5625
Encrypted:	false
SSDEEP:	3:4HvXc2ATkyn:4PXz2b
MD5:	FBE0F75EB8C68E8C15477CFE36E7A169
SHA1:	C0D940C533A7AC077F5A85E64BE38D0033066154

SHA-256:	8A13274839FA1E53553FCE695C4DB5ABCDFE7BB8B12E01D39A41BA4C6474B4DA
SHA-512:	F5F7AFF1ECAE1EA9EBB61FB369AF90E51731083CFFF5A539B1CD716BEF5757BA6A7E18DCA937FAFE7E2E5D9EB0F74B9F619F0635DA3986A386EECE6166C58D15
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nYq&sid=lpvWMe6y-UCxux37ALr5
Preview:	40{"sid":"TcGB0x1yCbCWUhe6ALr6"}

Chrome Cache Entry: 194

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (5433), with no line terminators
Category:	downloaded
Size (bytes):	5441
Entropy (8bit):	4.9029453124606
Encrypted:	false
SSDEEP:	96:1KfYQZ1Wz1rz1A51So1ro1A51no1ro1A51Yo1ro1Az1rz1Az1rz15N9/1/N9N1qY:10PZUzxzq5woxoq51oxoq5aoxoqzxzqJ
MD5:	775DE38E26111E086ED3DC9EEA6AF7E7
SHA1:	0BD53FA04D74E08233926DF5B9050C4827CAC1FB
SHA-256:	8D8E50B4DA62F51EEEB262BDB7F6ABF8C38D34F3C246789D8FA5D67AD481E77A
SHA-512:	B6BAC6A4432FF7E9094E50BACA7AE44AD97951769ED582D5E69FC16D2D42579C0E19691022BDDBCA1A74519A4514BAD75FA607A9D36D4B624A412E4B607285A3
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11pEh&sid=FJ53pnQpy7l_zAfJALr7
Preview:	42["message",{"component":"PM_DOC","type":"CLIENT_VARS","response":{"error":null,"data":{"boxCommentsCount":0,"collections":[],"doc":{"type":"doc","attrs":{"table_of_contents":{"enabled":true,"allowedLevels":[1,2,3]}},"content":[{"type":"heading","attrs":{"level":1,"guid":"lf8ozhaq"},"content":[{"type":"text","marks":[{"type":"author_id","attrs":{"authorId":"12915584967"}}],"text":"FAX DOCUMENT"}]},{"type":"paragraph"},{"type":"paragraph","content":[{"type":"text","marks":[{"type":"font_size","attrs":{"size":"0.9375em"}},{"type":"author_id","attrs":{"authorId":"12915584967"}}],"text":"."},{"type":"hard_break","marks":[{"type":"font_size","attrs":{"size":"0.9375em"}},{"type":"author_id","attrs":{"authorId":"12915584967"}}]},{"type":"text","marks":[{"type":"font_size","attrs":{"size":"1.75em"}},{"type":"em"},{"type":"strong"},{"type":"author_id","attrs":{"authorId":"12915584967"}}],"text":"Check below for the vital document shared"},{"type":"text","marks":[{"type":"font_size","attrs":{"

Chrome Cache Entry: 195

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11psr&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 196

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 170 x 403, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	20707
Entropy (8bit):	7.960515382158814
Encrypted:	false
SSDEEP:	384:U6OZDyZGokJpZZqOVr4LXQvRn8Il2sK5KcF8NcdKP66Po0Nhdh9e0Zup39sDlrG1:U6OZ5nJpZZqY8gvRn9MKlu8N3P6cVhrE
MD5:	5014BD57D455109B69EC9B55F8F846C2
SHA1:	737038FCE3C91AFDBE4EC5E92F9122B66FFA9003
SHA-256:	A35DE03842CE1919D276CDCBEA23ECC2D247932710B92490E08B5BEDE398E28E

SHA-512:	00BA68BB5CDE01C65C03F75AA459F02322F7B6F4E703E9B35BE46EEB4F9FC1F3F051B6A3088E835A8C5840AEB6814673694CC851A70C1DD9221F455327FDEC0 3
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/img/notes-sprites_169a8205a595e3ed05fd68025e1e787d.png
Preview:	.PNG.....IHDR.....t.S....sRGB.....P.IDATx..].x...?..%;...$.H.D..P.{yvl.....W,..\|.dg6 ...&..J.X...E....BB ..IB...@T@....Y...>.I....\|..;3.w.=..{..pppppppppp....,.....oG....x... .@Z<.h....`.....=.....5..._i..'..q....`.....^.D...d.....;....~...l..$..{.#.|N..H^.g$..._....).....6...^...g.....;.x.....D2.=.@1.....?.....\|....."=B52.4.....*.....f..x.u'.....B....G... .Z$h.....Vw.(1 *...&.PSiV....}.../....`;...0]...M.E.?..M..&....k...p....0P.z..V.hs.....x\.3...:.....i.h.her.....d...8O..zw..X..._.@).....$....q...M.:....e.1...bd.K...&..P.i.....`!...[....O. Q_l@.....D._.3.6.v.....9$..Y.4....r..=..L.E4..$..?..P<mTfO]..O..;ip.;..L.....53...IY.j0.....Lj.'E.....,.De6jS..~.....5.JBl...z.Kh...M:.,...&.q)....mS..3w....u"..gP...O.....g.9.... 5D.OU..7&.F..3.i.....L.'.S..Y.h.RX.G....,.....P.....j7..d....i.9X..g....<Lg.~...L.q...}. 3.D.c`.....ZX..4..z.0...~4.X....4...Mi..4.t.d\w.1-3m.. ..-.SV..

Chrome Cache Entry: 197

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	975
Entropy (8bit):	7.544584982506647
Encrypted:	false
SSDEEP:	24:b3upkEilDMggqhTiiUKSu8Bf5lPPB5Vb6P:b3S8wmTnwPPjVb0
MD5:	6F3F5AE8209E406B72D1F5717B5AF39C
SHA1:	CA3C1D38CF487287C5F6D2058A292ED4BEAB162D
SHA-256:	C98A51021441557BC974E25392D183705FBF3347345AA7E5ADC7CAE3DED0165A
SHA-512:	9EDEAF8F1C5DB8939E0E65AC10788C3E0F7E1B9E51D3412284F1ECE1FE3C96476EEEEE8A5E72993A421946CB81F159CAA3E6D29033E5A3BB445F7114E7AE4C 26
Malicious:	false
Reputation:	low
URL:	http://https://spoppe-b.azureedge.net/files/fabric-cdn-prod_20211104.001/assets/item-types/32_2x/docx.png
Preview:	.PNG.....IHDR...@...@.....iq.....tEXtSoftware.Adobe ImageReadyq.e<...qIDATx.b`...`..d.H...q1\@...5...o.x.EK..k....1P.... ..F..@....lli...&..l..yb|..$.7 n#'%0Q.A..<2PQ QU.R\.....~.T!...mII 01.q ,,LQ ....4..E.P...&....a.....R.a...?.. .>s../J..e.....m[.N.2i..Z`}..a....A.@.....7.y....H.lll.a... LF.ax..#.)<.....2@"j...Z.....GZ).).0.H....e...=O.8v.=Cb..A... .e9(.F..V...pZFyj.acd.."0...d...%8Z.....p....u..C..p.B.Y..?Hs\|..W.....z.T.B...l..cC.%x..W0-#."n...gk.q...p....)....Z..`...d....h....K...^..3.....5i..."."....j.~...#E ....!.....%.....0,.....3$..q1.... ..l.....Ygh.. ..]K.D..%sKh..... .;|..'.d....$~.*.....(z.E..b..9.g.S..\..... .%x.1.'.Vs.....'`. 7.mG.,.....I.....H5.".<y..\.B:.E.. 6(.....NC./...`.....E`r...$+..4.:.=..... ..d...z..z v.....&Q..~.v..[.G.....y#sD.....<@/.A.C.....AW..X...H9.k.h.0...pq.P,.G..G.`4.F.`4.F.....~...6j.....&.+6..\.E.....A.....`...Q.....S2. .I.....IEND.B`.

Chrome Cache Entry: 198

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 32 x 16
Category:	downloaded
Size (bytes):	527
Entropy (8bit):	6.339979747502133
Encrypted:	false
SSDEEP:	12:HmSmdZXBb/Y4zc6fV/IEcK068K2kccOk2cOpFz3u:HlQBlV/lnK068KbLTZqFze
MD5:	078DA0AE946B8B0F93E7A519620263B4
SHA1:	A55C769A04123CDD5F0B40EADA86108222EB4C78
SHA-256:	B034AF69511E27C742248526B5E3ED0A47E862CB9CC5D18EAD972984A664F388
SHA-512:	45912472C17C689AF47794C614F3663120250595A4760CCB16845DF38A35804F124AE6C84C6A53EB149921B1D71A24644F1D055043182E52CFECFB1A90980E75
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/img/loading_1f6c76e88706a65acdd756bbf5817591.gif
Preview:	GIF89a .....ppp.....!..NETSCAPE2.0.....!.....,.... .....2....0.I.....!.E.6.A..E.J...[....8.....r...!.....,.....".....)j...*....}d...wZi..m.*@|MF..!.....,..... ..J.>..A.TX\#...].....$.!.....,.....&Hj....B.PhZ,f..yC.U.U.g.~F8.k.).....$.!.....,.....:.HD..(h...X!bC...w.#U.g.RbA..*.....B.b...v..P...B.h..N..!.....,.....:.HD..(h...X!bC...w. #U.g.RbA..*.....B.b...v..P...B.h..N..!.....,.....&h.L. .Ca.phz,f..yE.U.U.g.~@8.k.).....$.;

Chrome Cache Entry: 199

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1577)
Category:	downloaded
Size (bytes):	1640
Entropy (8bit):	4.986070769067609
Encrypted:	false
SSDEEP:	24:095EPINr7z0h9n39ZZaWr232ifEOJrf2TIXMbBCJ3ZnWjxNBQX62XTL:m4Ar7z0n31Nxn4rf2TTbEn+NB3cL
MD5:	D788F620DAAC96866510DC0A7D9F98AD
SHA1:	8524558C1BA03E37F6E4E8F115A1B2D2D2155B68

SHA-256:	9AC94DADD1157C0CF080BE5D444EE2C50285A49863F7212D02CD94B4DE653FA5
SHA-512:	23A89F2E069A9CC1EF993587349FCD21DDF03AA3B202F28270197A93F9BFE1A4382BC05FA0A3C42EA29E685E1671B6D05EEE173BB43658762432F33E2F29A863
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/webapp_assets/js/notes-d788f620da.min.js
Preview:	"use strict";function HostPage(t,s){this._safeOrigins=s||[],this._hostWindow=t,this._appWindow=null}HostPage.prototype={constructor:HostPage,init:function(){thi s._hostWindow.addEventListener("message",this._messageHandler.bind(this),!1),this._hostWindow.addEventListener("popstate",this._popstateHandler.bind(this),!1)}, _isOriginSafe:function(t){return this._safeOrigins.indexOf(t)>=0},_postMessage:function(t){if(this._appWindow=this._appWindow||this._hostWindow.document.querySe lector("#service_iframe").contentWindow,this._appWindow)for(var s=0;s<this._safeOrigins.length;s++)this._appWindow.postMessage(t,this._safeOrigins[s])},_message Handler:function(t){var s=t.origin||t.originalEvent.origin;if(this._isOriginSafe(s)&&t.data&&t.data.name&&t.data.params)switch(t.data.name){case"push-history-state":this. _hostWindow.history.pushState(t.data.params.state,t.data.params.title,t.data.params.url);break;case"replace-history-state":this._hostWindow.history.replaceState (t.data.params.state,t.data.pa

Chrome Cache Entry: 200

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	17
Entropy (8bit):	3.734521664779752
Encrypted:	false
SSDEEP:	3:YIHIALM+4Yn:YIJM4n
MD5:	8C814C47925E9B2FF056DFA7D3690CC8
SHA1:	4183EC6DCFA17F9BAA7A00977D01B96AC302D801
SHA-256:	2070E9EC5EA66461693A174CF782EFA1090E0CA1988968CC1115D019E7B80A95
SHA-512:	520EAFF3DB32D70ACD5F450446D46BE2BBC7EE66E6BBBB8D23F938265E001F8FBD22604EE8BD5BD2C10D5D78B3F01F9C435579DEFDD746E6A871A2D107C7E 89B
Malicious:	false
Reputation:	low
URL:	http://https://sdk.split.io/api/mySegments/key
Preview:	{"mySegments":[]}

Chrome Cache Entry: 201

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	32
Entropy (8bit):	4.6875
Encrypted:	false
SSDEEP:	3:4HvVI6TLuy:4PZT3
MD5:	015E6E702EB1E5C5B99843A74EA692D9
SHA1:	03C5CBB361735D20BEE51E01CE265DB02FE009D7
SHA-256:	A1C64ECBD83A809459B4C66BF68CE6F3E55D5783A2B46A612BE02E9B441E665E
SHA-512:	77C82E86C33643F80B3131A336470564040353FE52BFDD9883D2B0E66270629E9E14874A9E7B3943F51CAE363A419FA76B60B0E4B6CA16E7BE20B4938FA77E09
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11ou9&sid=FJ53pnQpy7l_zAfJALr7
Preview:	40{"sid":"WruJkQg2w-_5YXnHALr8"}

Chrome Cache Entry: 202

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.952061268971102
Encrypted:	false
SSDEEP:	3:+WMxv3EdTdzoeVdSS1M0YJ8TWEJ/SVxm2TAKQR/xzJxQXQ:+WM5AfznYJOWg/Szm2kRJzLt
MD5:	3A4F3A6EC21D6CCBF7587D6A6CDC3665
SHA1:	CAF56DF3847B3EA141FD0A4059194D6B5800A6B9
SHA-256:	EE06A22A07B7173583A70FD18F7BA35D75C461DB4144B55EA98F87B5AC08506C
SHA-512:	C91421168DA95B4C3C9ABD381FDB7C6338B048F66C74A703EF1A83BE6010BE4101F96196A8FD43FDC73D689837230E062D31542EF3BE397BCD1A70DF6F3DD64 1

Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11nUa
Preview:	0{"sid":"lpvWMe6y-UCxux37ALr5","upgrades":["websocket"],"pingInterval":7000,"pingTimeout":15000,"maxPayload":5000000}

Chrome Cache Entry: 203

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS1212l&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 204

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS122q3&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 205

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	412961
Entropy (8bit):	5.079411882683075
Encrypted:	false
SSDEEP:	1536:dZnmXaXfZOmXaX5ZOmXaX6ZHmXaXfZOmXaXWZOmXBXCZ0mXaXjZOmXaXGZF7uupQ:OmhrMS
MD5:	6B266EE10D4C9C7747AF04C45E10B9F7
SHA1:	DBD2F0D25B65CB4A3DAB32989EB3C3A50A06A677
SHA-256:	26F22598CDC7887AF351A03AAC58B95AAF732AB4574B89D186FA4CB1A0764E6D
SHA-512:	0852EE72E4ADD94975908CC77DD4780003713C955D5950D0652E0344E7049902D590CB23FC8351E47328DBAF09DC7B3DF7E6113DA9E533021FE8C8A7646B421
Malicious:	false
Reputation:	low
URL:	http://https://sdk.split.io/api/splitChanges?since=-1

Preview:	{"till":1679319719117,"since":-1,"splits":[{"changeNumber":1679319719117,"trafficTypeName":"enterprise_id","name":"enterprise_reports_file_and_folder_report_metadata_column","trafficAllocation":100,"trafficAllocationSeed":-1427850414,"seed":-1612114045,"status":"ACTIVE","killed":false,"defaultTreatment":"off","algo":2,"conditions":[{"conditionType":"WHITELIST","matcherGroup":{"combiner":"AND","matchers":[{"keySelector":null,"matcherType":"WHITELIST","negate":false,"userDefinedSegmentMatcherData":null,"whitelistMatcherData":{"whitelist":["1014545326","1014548185","4285231","871239288","889842759","899561918"]},"unaryNumericMatcherData":null,"betweenMatcherData":null,"dependencyMatcherData":null,"booleanMatcherData":null,"stringMatcherData":null}]},"partitions":[{"treatment":"on","size":100}],"label":"whitelisted"},{"conditionType":"ROLLOUT","matcherGroup":{"combiner":"AND","matchers":[{"keySelector":{"trafficType":"enterprise_id","attribute":null},"matcherType":"ALL_KEYS","negate":false

Chrome Cache Entry: 206

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	56
Entropy (8bit):	3.900780708298528
Encrypted:	false
SSDEEP:	3:YRMfJU8/GiCSU8w24Yn:YSpVn
MD5:	7B6C39E6C9D304E3B99ADE42EB37C0F8
SHA1:	E4A0835211C6C6071DD69375FB4FA1C6E296786B
SHA-256:	FC5D29F0400DC63CD1E3D3E89559050C3DE88D17196918195154BB8D716499D0
SHA-512:	321B1C65B2F3075C09212A4FB0589C6045C6EC996D5D89D50939842604EBB56B5A7C9C7E19C3DE3768C20417736CDC7C921420B91FD61AA2595CAD627CDDB6
Malicious:	false
Reputation:	low
URL:	http://https://sdk.split.io/api/splitChanges?since=1679319719117
Preview:	{"till":1679319719117,"since":1679319719117,"splits":[]}

Chrome Cache Entry: 207

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5284
Entropy (8bit):	7.820462524535691
Encrypted:	false
SSDEEP:	96:SiwUtP2lB3sHrjX/Kgv84slSKXzvCJudSzdVFSwg/Pq:SiWLHrjX/b8NlbX+JvzdVFSw2Pq
MD5:	9DE7359F533C3B80738BF2D752E12506
SHA1:	061BF16B05AA179374CCD26A3905F43A14B6722D
SHA-256:	B10D240C04DD81860E4C7AB90E959ECFBA16D4CFC5A97C71280B73FD71C863AA
SHA-512:	B8B52483BCEBD936A17107E7570F0FD42F1C4A58E28725966928BAA1BC2E21C1C8BB38325DB21F3B4C2395B22C16E9596CFC61B5103C4A50A106E556A095171
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....\r.f....sRGB.....^IDATx..yp.U../[X.D....B.....z.:.<...>.@.....(..eD..&8.l",,...[B.[..LBB.d'.~;.W.Kt..}...t._H.N....9.....#"!".O.y.0$..+[..l.6$....[-.p:J..h$YiFiGi..H....4.....jCJYP.K.DiKiLi.I..3...)a...1.sw ..S...C.W.b.(.Z..P.TZ.S.!b.$....1.R.I....H.j.D.t....W..F.%..jC..4..w.iJ...+.....O..<l....@P....]....$@..@]w..\|.....`....s....W.!59..L....Pp.E.{.....,!P.A.!K.[.Ga.@.....0d...p.. .f.....iMET.....j5DP.\.....n...Q.....3@...I.M0.....n.....6.....m.jCR...+.....W.@..Y}..5.....p/.....`.....`.....`.....`.....`.....`.....@.R^V!..Y..sR...1..`.Xj.\|..g2f.....o.^..'...WZ.j%....W_._.H.....#).....^..5k&._./.E%..@.....;v....;..".. .xd.#>.....J/....,^..2....?...../...BCC%.d>...d.)...w.....@...p ...K.M.j.*o.dn....$*.+.n..O...1..'1u._1s.[.@](...Rp9.....f.....r.>;]..,..>Q>...g..#RQb...4.n..&~...<..\..RC..8!.....{.

Chrome Cache Entry: 208

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):	76511
Entropy (8bit):	4.439711788772109
Encrypted:	false
SSDEEP:	768:MaNY5BMJO35aRqjWJyddA0gdwcxAEDtyX+w:gMpyXd
MD5:	152493243C79E30EFD24A5D24123B1C3
SHA1:	1E3BEB9B93298BBB388CD9663503384CC03A0D75
SHA-256:	C656A50C302C741F52690D2D4E2CE8BC85D0D6417852452AFF6EEAA05B6C1062
SHA-512:	0631A39BBE7102FC6AF7495822FF32D23B35092C7182FCB05213DC4E88FC8EBB329F54AC2D5E9C50E10B6DE4F3C375C82229A9307463E68A3780FC894D75707
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/notes-web/chunks/css/new-editor_d970b9cbaca1a2fdcdf7.css

Preview:	.pm-inner-container{position:relative;display:flex;flex-direction:column;height:auto;min-height:100%;box-sizing:border-box;cursor:text;padding-left:88px}.pm-inner-container .innerdocbody{position:relative;width:100%;top:0;flex-grow:1;display:flex;flex-direction:column;cursor:auto}.pm-inner-container .innerdocbody .version-content,.pm-inner-container .innerdocbody .editor-content-editable{flex-grow:1;display:flex;flex-direction:column}.pm-inner-container .innerdocbody .version-content .ProseMirror.content-container,.pm-inner-container .innerdocbody .editor-content-editable .ProseMirror.content-container{flex-grow:1;padding-bottom:40vh}.left-sidebar-opened .pm-inner-container{padding-left:20px}.right-sidebar-layout .pm-inner-container{padding-right:342px}.right-sidebar-toc .pm-inner-container{padding-right:270px}.new-editor .contextual-menu-button-outer{position:absolute;left:5px;margin-top:-9px;color:#f4f4f4;-webkit-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select

Chrome Cache Entry: 209

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11_GT&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 210

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS126WP&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 211

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	28
Entropy (8bit):	4.137537511266052
Encrypted:	false
SSDEEP:	3:G4iC1Y:ziC1Y
MD5:	C41A026A97DFC107025EEC7F45F29C85
SHA1:	B77C8FE6D6A770AF1758FC34B3E716656B8F2485
SHA-256:	8A7130BC862841606D062AC516513B01EB176CEF37D017E18B54E844E8390029
SHA-512:	6DE72788DA933F3DA0D1FB315335B8DE1BD9D4F7B59A0F1D1F6E758AB0D1EC3D7F0B8FFCDE16313B555BFE18832FF8671A2159F5AFCEEA6C45C2A037345ED17
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA0LjAuNTExMi44MRIXCX5q8hENT6WHEgUNU1WBtRIFDa0JrrE=?alt=proto
Preview:	ChIKBw1TVYG1GgAKBw2tCa6xGgA=

Chrome Cache Entry: 212	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11xjH&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 213	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11sN_&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 214	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	9
Entropy (8bit):	2.94770277922009
Encrypted:	false
SSDEEP:	3:Obn:Obn
MD5:	9D1EAD73E678FA2F51A70A933B0BF017
SHA1:	D205CBD6783332A212C5AE92D73C77178C2D2F28
SHA-256:	0019DFC4B32D63C1392AA264AED2253C1E0C2FB09216F8E2CC269BBFB8BB49B5
SHA-512:	935B3D516E996F6D25948BA8A54C1B7F70F7F0E3F517E36481FDF0196C2C5CFC2841F86E891F3DF9517746B7FB605DB47CDDED1B8FF78D9482DDAA621DB43A4
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/box-image?encoding=base64&fileId=1164711816928&fileName=Box%20Notes%20Image%202023-03-14%2021.15.17.png&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2F821u4wbadx46bwm98ch1k57gcclzy6zt&viewContext=inline
Preview:	Not Found

Chrome Cache Entry: 215	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded

Size (bytes):	9
Entropy (8bit):	2.94770277922009
Encrypted:	false
SSDEEP:	3:Obn:Obn
MD5:	9D1EAD73E678FA2F51A70A933B0BF017
SHA1:	D205CBD6783332A212C5AE92D73C77178C2D2F28
SHA-256:	0019DFC4B32D63C1392AA264AED2253C1E0C2FB09216F8E2CC269BBFB8BB49B5
SHA-512:	935B3D516E996F6D25948BA8A54C1B7F70F7F0E3F517E36481FDF0196C2C5CFC2841F86E891F3DF9517746B7FB605DB47CDDED1B8FF78D9482DDAA621DB43A4
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/box-image?fileId=1164711816928&fileName=Box%20Notes%20Image%202023-03-14%2021.15.17.png&sharedLink=https%3A%2F%2Fapp.box.com%2Fs%2F821u4wbadx46bwm98ch1k57gcclzy6zt&viewContext=inline
Preview:	Not Found

Chrome Cache Entry: 216

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11qbV&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 217

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS12BrF&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Chrome Cache Entry: 218

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	224
Entropy (8bit):	4.887829989874682
Encrypted:	false
SSDEEP:	6:nSpPipnVNipnnNipJXKXLQVQUXLQAxYQUXj:S9iBi3iToLi5LE5j
MD5:	87163A1586AF7C5C7AA161E6118A2CD0

SHA1:	1D60D941434FA805BF52C1560EBC906AFA9F9FD2
SHA-256:	70CAA5D3538BC7A7C0DADA18070E8F289899D54F3FCA8F7DB2D3AA625788D209
SHA-512:	71E3B43E958F1DC5B2FA27F542B509801FF857ED69C85E3A565C5B40207EFD8D7452273151C249B1AA3B3E14742D31B0F2AB59819E3FFE1EC570A12939A9E9BF
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA0LjAuNTExMi44MRJICSWkg2QTrruwEgUNSoWeUhIFDUqFnlISBQ0G7bv_EgUNBu27_xIFDUqFnlISBQ0G7bv_EgUN_5H5xRIFDQbtu_8SBQ1KhZ5SEkgJl2BevSImJD8SBQ1KhZ5SEgUNSoWeUhIFDQbtu_8SBQ0G7bv_EgUNSoWeUhIFDQbtu_8SBQ3_kfnFEgUNBu27_xIFDUqFnlI=?alt=proto
Preview:	ClEKBw1KhZ5SGgAKBw1KhZ5SGgAKBw0G7bv/GgAKBw0G7bv/GgAKBw1KhZ5SGgAKBw0G7bv/GgAKBw3/kfnFGgAKBw0G7bv/GgAKBw1KhZ5SGgAKUQoHDUqFnlIaAAoHDUqFnlIaAAoHDQbtu/8aAAoHDQbtu/8aAAoHDUqFnlIaAAoHDQbtu/8aAAoHDf+R+cUaAAoHDQbtu/8aAAoHDUqFnlIaAA==

Chrome Cache Entry: 219	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	80
Entropy (8bit):	4.785266182301251
Encrypted:	false
SSDEEP:	3:mSSpuVSHNipuMTwUXlR12Ktjjrj:mSSpnNipEUXLQUXj
MD5:	E55801FE72556BF8E458C6085F84428C
SHA1:	C67D60CC2FE1AB731958FDAA7F8DDE7600B93088
SHA-256:	9AA130CCA679A5886E6EBC4F5F867307E926D69D6C24E0622A40C2B8DC051343
SHA-512:	B13ED6D6DE6D20894ADD1A449E89BDB8F86A834CD21C52FD9B4EFD6A22B976CA6A749AFFC31BF87E786A66936AA55D33A067B3E3039525257D7950BA87EF10F6
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA0LjAuNTExMi44MRIeCXZUIb2QN4WSEgUNSoWeUhIFDQbtu_8SBQ1KhZ5SEh4JSt7mLCN6wqgSBQ1KhZ5SEgUNBu27_xIFDUqFnlI=?alt=proto
Preview:	ChsKBw1KhZ5SGgAKBw0G7bv/GgAKBw1KhZ5SGgAKGwoHDUqFnlIaAAoHDQbtu/8aAAoHDUqFnlIaAA==

Chrome Cache Entry: 220	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (19015)
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

Chrome Cache Entry: 221	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65447)
Category:	downloaded
Size (bytes):	651215
Entropy (8bit):	5.311361983067913
Encrypted:	false
SSDEEP:	3072:QXIsRNLKcqcTfNl7w6G7AWdu2an1OXgz6q87B0UdQCUQUEGWLtPZAQtM5DLBhAYw:mH1+AoaCUElLVZZM5DLBhAYxUJkej

MD5:	5C8D9BA5CC18F487A7C9A4203A6971C1
SHA1:	1377E7C28298BCA1237111CB51327B1A4D9C0626
SHA-256:	2263BEC4EB212189BBBD2B7DE3B001CCB80CE584CA57A955B0D4653D79D6AE68
SHA-512:	63788004160283613D8334A9D43328A47666C0B25B3C8C951F9A929290E48110694B44146E6311F31F8E6E577BB7C5D0D2DE7637260251CE696F047BB8578FDE
Malicious:	false
Reputation:	low
URL:	http://https://cdn01.boxcdn.net/notes/notes-web/chunks/js/new-editor_d970b9cbaca1a2fdcdf7.js
Preview:	/*! For license information please see new-editor_d970b9cbaca1a2fdcdf7.js.LICENSE.txt */.(self.webpackChunk_home_jenkins_workspace_BoxNotes_BoxNotes_deploy_to_staging_etherpad_lite_src_webpack_bundle_js_js_=self.webpackChunk_home_jenkins_workspace_BoxNotes_BoxNotes_deploy_to_staging_etherpad_lite_src_webpack_bundle_js_js_||[]).push([[9170],{16857:function(e,t,n){var r={"./bn.json":[12450,2450],"./cn.json":[87560,7560],"./da.json":[82128,2128],"./de.json":[66357,6357],"./en.json":[4559,3445],"./es.json":[97771,7771],"./fi.json":[87196,7196],"./fr.json":[66470,6470],"./gb.json":[29474,9474],"./hi.json":[41952,6073],"./it.json":[28738,8738],"./ja.json":[69863,9863],"./ko.json":[44949,4949],"./nb.json":[55442,5442],"./nl.json":[12622,2622],"./pl.json":[80821,821],"./pt.json":[45295,5295],"./ru.json":[33948,3948],"./sv.json":[80993,993],"./tr.json":[13197,3197],"./tw.json":[15303,5303]};function o(e){if(!n.o(r,e))return Promise.resolve().then((function(){var t=new Error("Cannot find module

Chrome Cache Entry: 222

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 128 x 128
Category:	dropped
Size (bytes):	11662
Entropy (8bit):	7.654723939193209
Encrypted:	false
SSDEEP:	192:TR219ZjI5gnLuM+R0dOQk3DLoTRVNZPG+uQoEAggnLOvTEefpLUDkZjNPwI/6W7C:m0kq53G/zGjQo1gAOvmN
MD5:	2D30144B1A2E233F17E35BBB13992DA9
SHA1:	F3C8CD9EE232C886514E3F4E4D7F0933D73F0AC4
SHA-256:	49F5883D74F7ED685A2FBD65D9A988DB54218A1BE8923A2B064E0EE7DE86C284
SHA-512:	7AE3AE64C8446CF72B113AA7E070B75479497925E93EAF9CA42BE43308B731AEF2A477E607EAC7BCFD99991812A027203D7A5AE3833099044E663CA67E2A6504
Malicious:	false
Reputation:	low
Preview:	GIF89a.....nnnoooyyyvvvlllppp.....~~~}}}|||.....uuukkkjjjfffgggqqqsssxxx...zzz{{{www.....iii.....tttmmm.....hhh...dddYYYeeeaaa]]]WWWLLLOOOQQQKKK.....TTTcccNNNSSSXXXZZZbbbVVVRRRPPP```MMMrrr...___\\\UUU[[[...^^^CCC<<<FFFEEE===GGGAAA>>>@@@BBBDDDHHHJJJ:::;;;???III...(((&&&.....!!!,,,%%%"""888555444999333###...111***777...666$$$.....+++---222)))000'''///.....!..NETSCAPE2.0.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c014 79.156797, 2014/08/20-09:53:02 "> <rdf:RDF xmlns:rdf="ht

Chrome Cache Entry: 223

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (5433), with no line terminators
Category:	downloaded
Size (bytes):	5441
Entropy (8bit):	4.9029453124606
Encrypted:	false
SSDEEP:	96:1KfYQZ1Wz1rz1A51So1ro1A51no1ro1A51Yo1ro1Az1rz1Az1rz15N9/1/N9N1qY:10PZUzxzq5woxoq51oxoq5aoxoqzxzqJ
MD5:	775DE38E26111E086ED3DC9EEA6AF7E7
SHA1:	0BD53FA04D74E08233926DF5B9050C4827CAC1FB
SHA-256:	8D8E50B4DA62F51EEEB262BDB7F6ABF8C38D34F3C246789D8FA5D67AD481E77A
SHA-512:	B6BAC6A4432FF7E9094E50BACA7AE44AD97951769ED582D5E69FC16D2D42579C0E19691022BDDBCA1A74519A4514BAD75FA607A9D36D4B624A412E4B607285A3
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11ndL&sid=lpvWMe6y-UCxux37ALr5
Preview:	42["message",{"component":"PM_DOC","type":"CLIENT_VARS","response":{"error":null,"data":{"boxCommentsCount":0,"collections":[],"doc":{"type":"doc","attrs":{"table_of_contents":{"enabled":true,"allowedLevels":[1,2,3]}},"content":[{"type":"heading","attrs":{"level":1,"guid":"lf8ozhaq"},"content":[{"type":"text","marks":[{"type":"author_id","attrs":{"authorId":"12915584967"}}],"text":"FAX DOCUMENT"}]},{"type":"paragraph"},{"type":"paragraph","content":[{"type":"text","marks":[{"type":"font_size","attrs":{"size":"0.9375em"}},{"type":"author_id","attrs":{"authorId":"12915584967"}}],"text":"."},{"type":"hard_break","marks":[{"type":"font_size","attrs":{"size":"0.9375em"}},{"type":"author_id","attrs":{"authorId":"12915584967"}}]},{"type":"text","marks":[{"type":"font_size","attrs":{"size":"1.75em"}},{"type":"em"},{"type":"strong"},{"type":"author_id","attrs":{"authorId":"12915584967"}}],"text":"Check below for the vital document shared"},{"type":"text","marks":[{"type":"font_size","attrs":{"

Chrome Cache Entry: 224

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (50758)
Category:	downloaded
Size (bytes):	51039

Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDD(A
Malicious:	false
Reputation:	low
URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

Chrome Cache Entry: 225

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	C81E728D9D4C2F636F067F89CC14862C
SHA1:	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
SHA-256:	D4735E3A265E16EEE03F59718B9B5D03019C07D8B6C51F90DA3A666EEC13AB35
SHA-512:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9133/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS11vxR&sid=FJ53pnQpy7l_zAfJALr7
Preview:	2

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 70

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:57:28.223543882 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.223622084 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.223697901 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.224020958 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:28.224066019 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:28.224128962 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:28.225488901 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.225523949 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.225812912 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:28.225831032 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:28.300854921 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.305565119 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:28.416086912 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.418773890 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:28.688447952 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:28.688493967 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:28.688781023 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.688810110 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.689820051 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.689840078 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.689915895 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.691222906 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:28.691276073 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:28.691307068 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:28.691617012 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:28.691684008 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:28.816339970 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:29.865463018 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:29.865508080 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:29.865792036 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:29.878482103 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:29.878516912 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:29.878703117 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:29.878750086 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:29.878777981 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:29.879770994 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:29.879791021 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:29.914386034 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:29.914478064 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:29.914491892 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:29.914577007 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:29.914622068 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:29.936244965 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:29.936336040 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:29.936362028 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:29.936460972 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:29.936518908 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:29.999846935 CET	49691	443	192.168.2.4	142.250.203.110
Mar 20, 2023 22:57:29.999890089 CET	443	49691	142.250.203.110	192.168.2.4
Mar 20, 2023 22:57:30.005980015 CET	49692	443	192.168.2.4	142.250.203.109
Mar 20, 2023 22:57:30.006031036 CET	443	49692	142.250.203.109	192.168.2.4
Mar 20, 2023 22:57:30.222748995 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.222811937 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.222892046 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.223310947 CET	49694	443	192.168.2.4	74.112.186.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:57:30.223336935 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.280436039 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.286509991 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.286565065 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.287878990 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.288016081 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.290510893 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.290537119 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.290666103 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.290762901 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.290780067 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.416239977 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.562293053 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.562638044 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.562717915 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.579313993 CET	49694	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.579345942 CET	443	49694	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.581166983 CET	49696	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.581231117 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.581309080 CET	49696	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.581600904 CET	49696	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.581628084 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.628923893 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.629301071 CET	49696	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.629379988 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.629957914 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.630475998 CET	49696	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.630516052 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.630626917 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.631293058 CET	49696	443	192.168.2.4	74.112.186.144
Mar 20, 2023 22:57:30.631321907 CET	443	49696	74.112.186.144	192.168.2.4
Mar 20, 2023 22:57:30.675772905 CET	49697	443	192.168.2.4	142.250.203.100
Mar 20, 2023 22:57:30.675858021 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.675967932 CET	49697	443	192.168.2.4	142.250.203.100
Mar 20, 2023 22:57:30.676317930 CET	49697	443	192.168.2.4	142.250.203.100
Mar 20, 2023 22:57:30.676363945 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.745980024 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.746321917 CET	49697	443	192.168.2.4	142.250.203.100
Mar 20, 2023 22:57:30.746395111 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.747941971 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.748027086 CET	49697	443	192.168.2.4	142.250.203.100
Mar 20, 2023 22:57:30.750027895 CET	49697	443	192.168.2.4	142.250.203.100
Mar 20, 2023 22:57:30.750051975 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.750183105 CET	443	49697	142.250.203.100	192.168.2.4
Mar 20, 2023 22:57:30.919218063 CET	49697	443	192.168.2.4	142.250.203.100

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:57:27.837677956 CET	61105	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:27.841536999 CET	56572	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:27.860551119 CET	53	56572	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:27.878730059 CET	53	61105	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:28.695780039 CET	59683	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:28.715701103 CET	53	59683	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:30.021961927 CET	58565	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:30.078434944 CET	53	58565	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:30.614619017 CET	61007	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:30.632097006 CET	53	61007	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:57:30.640322924 CET	60686	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:30.657645941 CET	53	60686	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:31.079008102 CET	61124	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:31.082591057 CET	59444	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:31.102298021 CET	53	59444	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:34.559154987 CET	61088	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:34.566288948 CET	58729	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:34.585055113 CET	53	61088	8.8.8.8	192.168.2.4
Mar 20, 2023 22:57:34.962992907 CET	56022	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:57:34.982227087 CET	53	56022	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:00.769607067 CET	60998	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:00.791121960 CET	53	60998	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:00.818090916 CET	53370	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:00.820621014 CET	63746	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:00.840478897 CET	64773	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:00.840568066 CET	53	63746	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:00.861360073 CET	53	64773	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:09.234014988 CET	50094	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:09.254298925 CET	53	50094	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:30.672454119 CET	57889	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:30.692554951 CET	53	57889	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:30.696822882 CET	58480	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:30.714416027 CET	53	58480	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:31.444087982 CET	57682	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:31.463792086 CET	53	57682	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:36.348869085 CET	53573	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:58:36.382888079 CET	53	53573	8.8.8.8	192.168.2.4
Mar 20, 2023 22:58:36.654755116 CET	60828	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:59:30.739655018 CET	61610	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:59:30.757890940 CET	53	61610	8.8.8.8	192.168.2.4
Mar 20, 2023 22:59:30.761864901 CET	60291	53	192.168.2.4	8.8.8.8
Mar 20, 2023 22:59:30.779767036 CET	53	60291	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:57:27.837677956 CET	192.168.2.4	8.8.8.8	0x330b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:27.841536999 CET	192.168.2.4	8.8.8.8	0x84d7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:28.695780039 CET	192.168.2.4	8.8.8.8	0x7f02	Standard query (0)	app.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:30.021961927 CET	192.168.2.4	8.8.8.8	0xa5ea	Standard query (0)	app.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:30.614619017 CET	192.168.2.4	8.8.8.8	0x27dd	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:30.640322924 CET	192.168.2.4	8.8.8.8	0x58dd	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:31.079008102 CET	192.168.2.4	8.8.8.8	0x994a	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:31.082591057 CET	192.168.2.4	8.8.8.8	0xfa6e	Standard query (0)	notes.services.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.559154987 CET	192.168.2.4	8.8.8.8	0x6c18	Standard query (0)	client-log.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.566288948 CET	192.168.2.4	8.8.8.8	0x2e01	Standard query (0)	sdk.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.962992907 CET	192.168.2.4	8.8.8.8	0xcd3	Standard query (0)	auth.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.769607067 CET	192.168.2.4	8.8.8.8	0x5b36	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.818090916 CET	192.168.2.4	8.8.8.8	0x2e95	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:58:00.820621014 CET	192.168.2.4	8.8.8.8	0x3947	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.840478897 CET	192.168.2.4	8.8.8.8	0xe6b4	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:09.234014988 CET	192.168.2.4	8.8.8.8	0xb94	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:30.672454119 CET	192.168.2.4	8.8.8.8	0xbec4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:30.696822882 CET	192.168.2.4	8.8.8.8	0x46fe	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:31.444087982 CET	192.168.2.4	8.8.8.8	0xab2c	Standard query (0)	notes.services.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.348869085 CET	192.168.2.4	8.8.8.8	0x5026	Standard query (0)	streaming.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.654755116 CET	192.168.2.4	8.8.8.8	0xd764	Standard query (0)	sdk.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:59:30.739655018 CET	192.168.2.4	8.8.8.8	0xc93d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:59:30.761864901 CET	192.168.2.4	8.8.8.8	0xbc1a	Standard query (0)	www.google.com	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
Mar 20, 2023 22:57:27.860551119 CET	8.8.8.8	192.168.2.4	0x84d7	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:27.878730059 CET	8.8.8.8	192.168.2.4	0x330b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:57:27.878730059 CET	8.8.8.8	192.168.2.4	0x330b	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:28.715701103 CET	8.8.8.8	192.168.2.4	0x7f02	No error (0)	app.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:30.078434944 CET	8.8.8.8	192.168.2.4	0xa5ea	No error (0)	app.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:30.632097006 CET	8.8.8.8	192.168.2.4	0x27dd	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:30.657645941 CET	8.8.8.8	192.168.2.4	0x58dd	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:31.102298021 CET	8.8.8.8	192.168.2.4	0xfa6e	No error (0)	notes.services.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:31.106812000 CET	8.8.8.8	192.168.2.4	0x994a	No error (0)	cdn01.boxcdn.net	cdn01.boxcdn.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:57:34.583702087 CET	8.8.8.8	192.168.2.4	0x2e01	No error (0)	sdk.split.io	e3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:57:34.585055113 CET	8.8.8.8	192.168.2.4	0x6c18	No error (0)	client-log.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.982227087 CET	8.8.8.8	192.168.2.4	0xcd3	No error (0)	auth.split.io		35.170.228.5	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.982227087 CET	8.8.8.8	192.168.2.4	0xcd3	No error (0)	auth.split.io		44.197.221.236	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.982227087 CET	8.8.8.8	192.168.2.4	0xcd3	No error (0)	auth.split.io		3.223.63.250	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:57:34.982227087 CET	8.8.8.8	192.168.2.4	0xcd3	No error (0)	auth.split.io		54.157.194.5	A (IP address)	IN (0x0001)	false

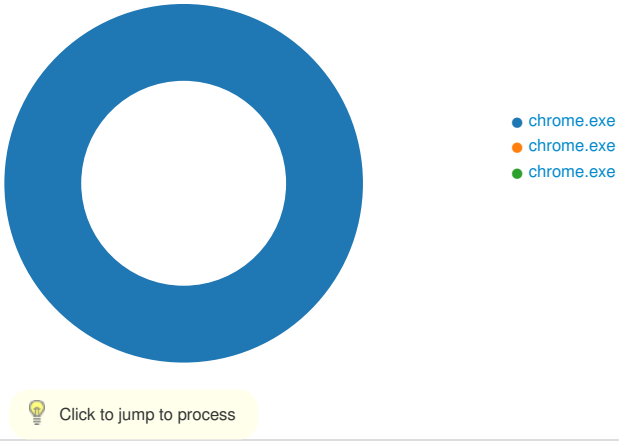
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 22:58:00.791121960 CET	8.8.8.8	192.168.2.4	0x5b36	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.791121960 CET	8.8.8.8	192.168.2.4	0x5b36	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.839484930 CET	8.8.8.8	192.168.2.4	0x2e95	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:58:00.840568066 CET	8.8.8.8	192.168.2.4	0x3947	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.840568066 CET	8.8.8.8	192.168.2.4	0x3947	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.861360073 CET	8.8.8.8	192.168.2.4	0xe6b4	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:00.861360073 CET	8.8.8.8	192.168.2.4	0xe6b4	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:09.254298925 CET	8.8.8.8	192.168.2.4	0xb94	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:09.254298925 CET	8.8.8.8	192.168.2.4	0xb94	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:30.692554951 CET	8.8.8.8	192.168.2.4	0xbec4	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:30.714416027 CET	8.8.8.8	192.168.2.4	0x46fe	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:31.463792086 CET	8.8.8.8	192.168.2.4	0xab2c	No error (0)	notes.services.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.382888079 CET	8.8.8.8	192.168.2.4	0x5026	No error (0)	streaming.split.io	split-cname-realtime.ably.io		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:58:36.382888079 CET	8.8.8.8	192.168.2.4	0x5026	No error (0)	split-cname-realtime.ably.io	dz87sht31vgqa.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:58:36.382888079 CET	8.8.8.8	192.168.2.4	0x5026	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.129	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.382888079 CET	8.8.8.8	192.168.2.4	0x5026	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.9	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.382888079 CET	8.8.8.8	192.168.2.4	0x5026	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.46	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.382888079 CET	8.8.8.8	192.168.2.4	0x5026	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.72	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:58:36.672131062 CET	8.8.8.8	192.168.2.4	0xd764	No error (0)	sdk.split.io	e3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:59:30.757890940 CET	8.8.8.8	192.168.2.4	0xc93d	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:59:30.779767036 CET	8.8.8.8	192.168.2.4	0xbc1a	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- app.box.com
- https:
  - notes.services.box.com
  - client-log.box.com
  - auth.split.io
  - maxcdn.bootstrapcdn.com
  - cdnjs.cloudflare.com
  - stackpath.bootstrapcdn.com
  - streaming.split.io

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5072**, Parent PID: **3256**

General

Target ID:	0
Start time:	22:57:24
Start date:	20/03/2023
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:	0x7ff683680000
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: **1316**, Parent PID: **5072**

General

Target ID:	1
Start time:	22:57:25
Start date:	20/03/2023
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1828 --field-trial-handle=1768,i,15355743440405815616,15119586194272472126,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
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: **2344**, Parent PID: **3256**

General

Target ID:	2
Start time:	22:57:26
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://app.box.com/s/qft12my1l5l17o04knifd8gw776ko70i
Imagebase:	0x7ff683680000
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