ID: 830976
Cookbook: browseurl.jbs
Time: 22:02:03
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

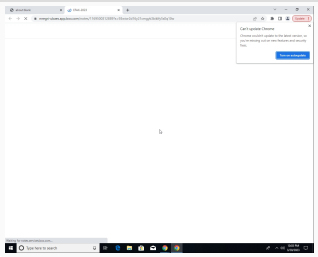
Windows Analysis Report

https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w

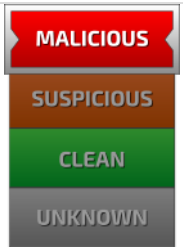
Overview

General Information

Sample URL:	http://https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w
Analysis ID:	830976
Infos:	



Detection



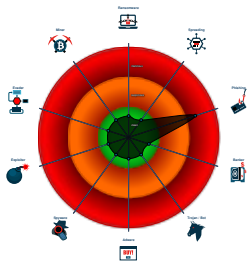
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish54
- Antivirus detection for URL or domain
- Phishing site detected (based on im…
- HTML body contains low number of …
- Found iframes
- No HTML title found
- Submit button contains javascript call

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6080 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5136 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1828 --field-trial-handle=1820,i,8349816860566181976,9620813474687927870,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5544 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
43432.5.pages.csv	JoeSecurity_HtmlPhish_54	Yara detected HtmlPhish_54	Joe Security	
89623.6.pages.csv	JoeSecurity_HtmlPhish_54	Yara detected HtmlPhish_54	Joe Security	
95241.9.pages.csv	JoeSecurity_HtmlPhish_54	Yara detected HtmlPhish_54	Joe Security	
89623.14.pages.csv	JoeSecurity_HtmlPhish_54	Yara detected HtmlPhish_54	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing

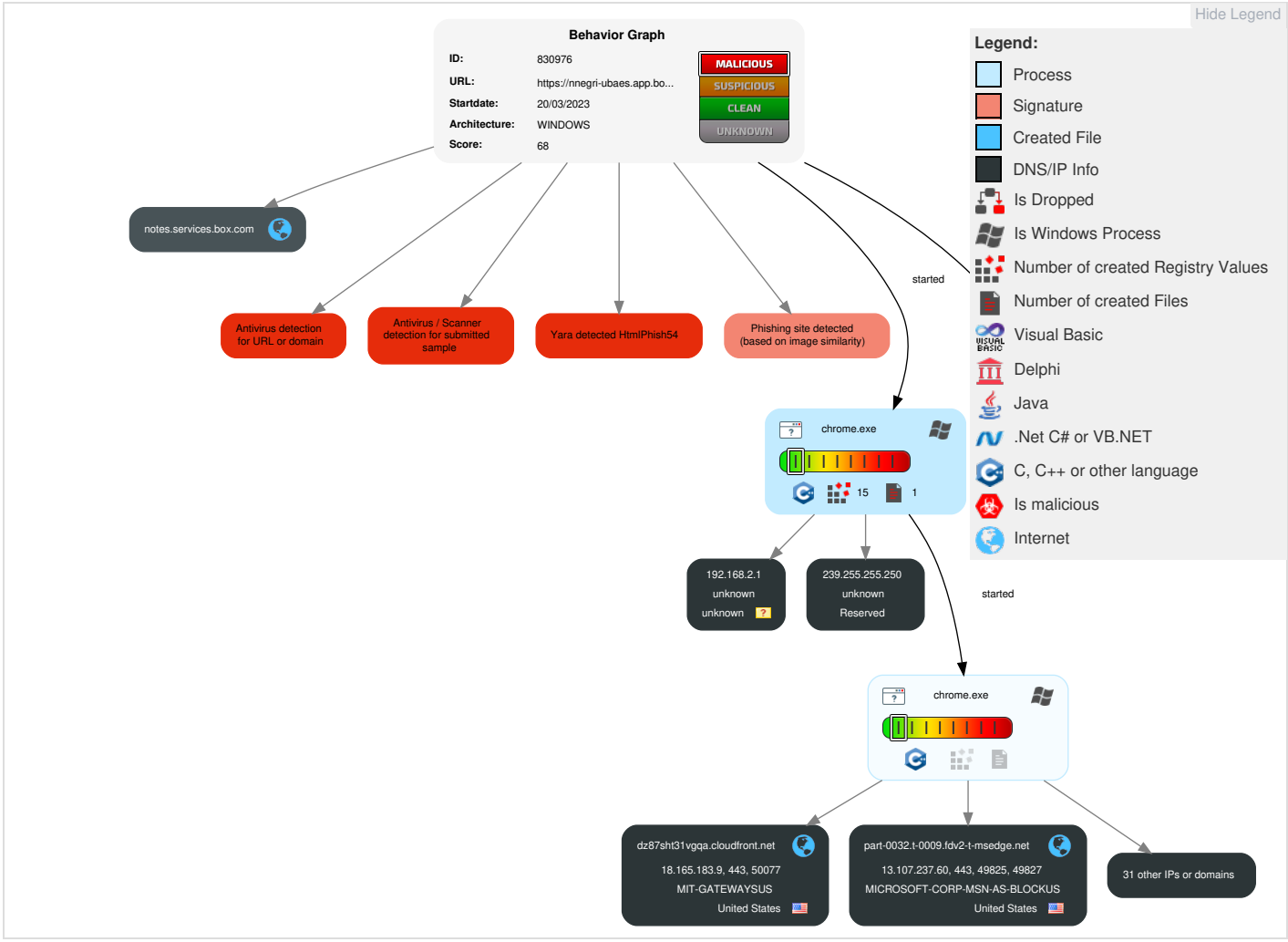
Yara detected HtmlPhish54

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
1 Drive-by Compromise	1 Scripting	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)	1 Scripting	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

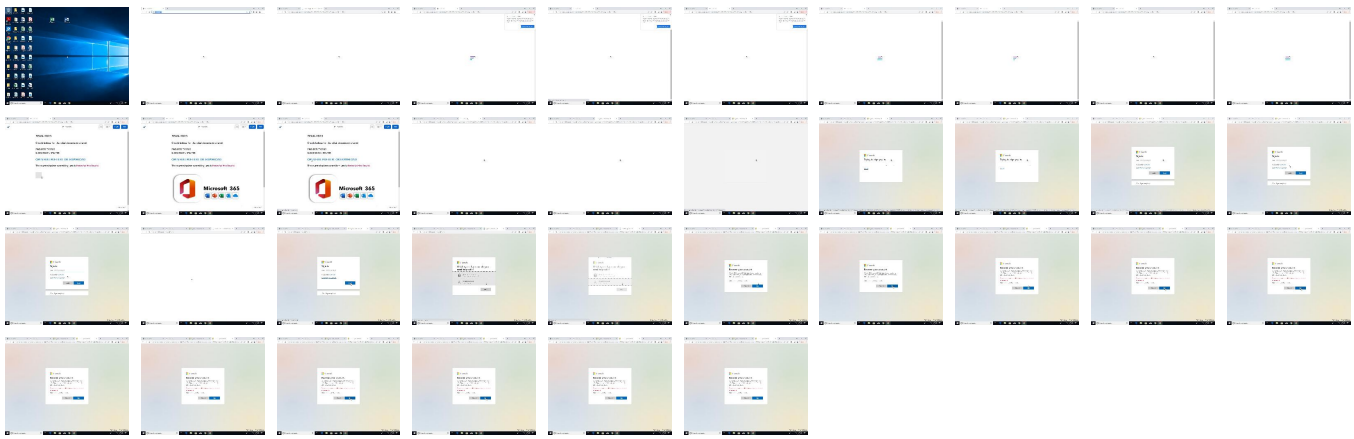
Behavior Graph

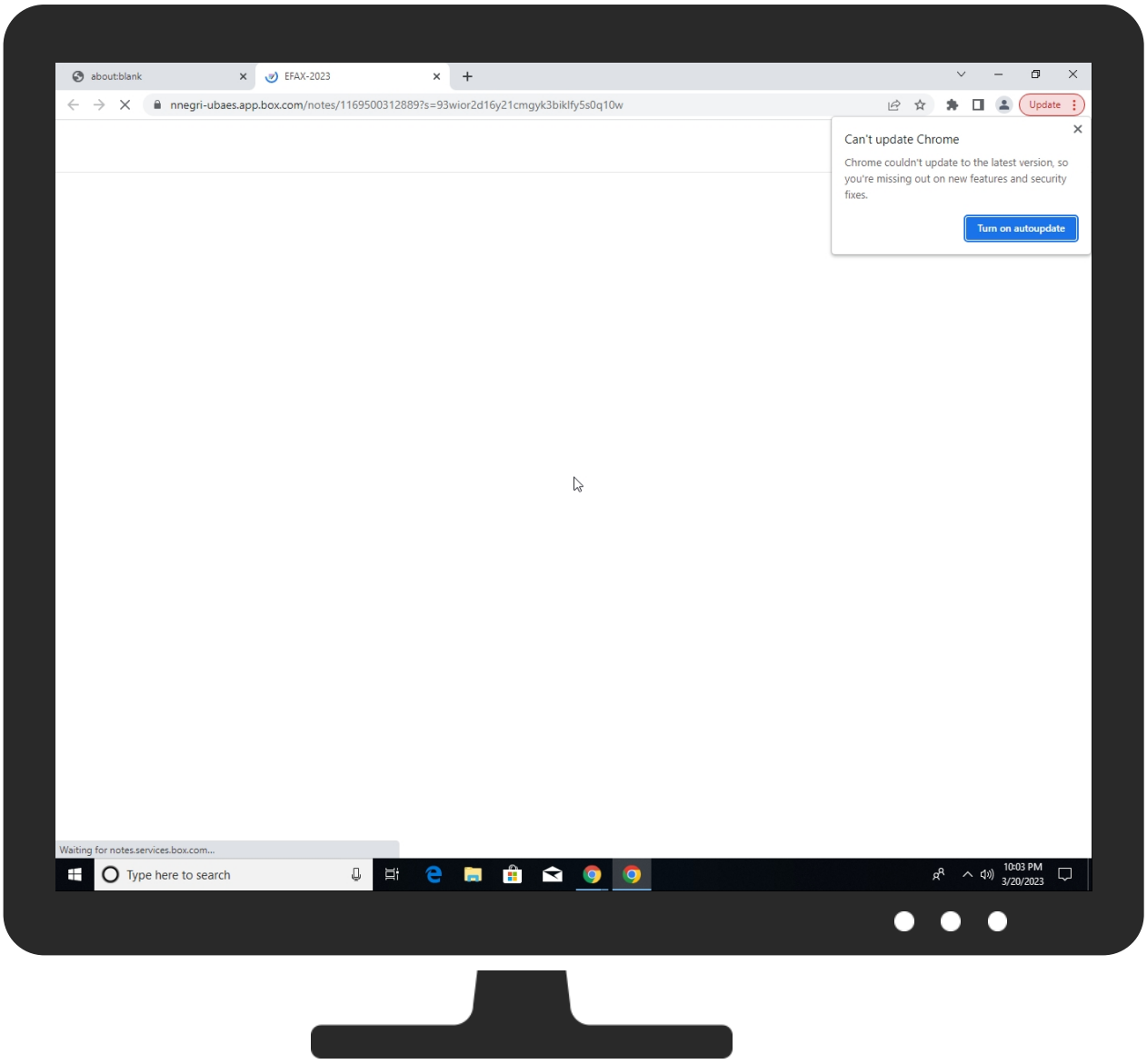


Screenshots

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://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w	NaN%	Virustotal		Browse
http://https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w	0%	Avira URL Cloud	safe	
http://https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://notes.services.box.com/p/note?fileId=1169500312889&hostname=nnegri-ubaes.app.box.com&sharedLink=https://nnegri-ubaes.box.com/s/93wior2d16y21cmgyk3biklfy5s0q10w	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://capitaltltleandescrow.net/?oxhv	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://angular-ui.github.io/bootstrap/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://capitaltltleandescrow.net/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nnegri-ubaes.app.box.com	74.112.186.144	true	false		high
auth.split.io	44.197.221.236	true	false		high
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
accounts.google.com	142.250.203.109	true	false		high
notes.services.box.com	74.112.186.144	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false		unknown
HHN-efz.ms-acdc.office.com	52.98.241.162	true	false		high
capitaltltleandescrow.net	23.227.196.212	true	false		unknown
www.google.com	142.250.203.100	true	false		high
part-0032.t-0009.fdv2-t-msedge.net	13.107.237.60	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
client-log.box.com	74.112.186.144	true	false		high
dz87sht31vgqa.cloudfront.net	18.165.183.9	true	false		high
www.office.com	unknown	unknown	false		high
sdk.split.io	unknown	unknown	false		high
r4.res.office365.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
account.live.com	unknown	unknown	false		high
cdn01.boxcdn.net	unknown	unknown	false		unknown
outlook.office365.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
identity.nel.measure.office.net	unknown	unknown	false		high
portal.microsoftonline.com	unknown	unknown	false		high
streaming.split.io	unknown	unknown	false		high
clientlog.portal.office.com	unknown	unknown	false		high
acctcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZDcK&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZDkn&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZG8i&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/client_log	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZNyY&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZKin&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://www.office.com/prefetch/prefetch	false		high
http://https://outlook.office365.com/owa/prefetch.aspx	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZWhm&sid=bafhQb8Iuy6TyutvAC5k	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZZVI&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZNde&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZdmN&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2Ze2O&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZLqy&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZWgd&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZadP&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/box-image?encoding=base64&fileId=1169506039580&fileName=Box%20Notes%20Image%202023-03-20%2010.57.19.png&sharedLink=https%3A%2F%2Fnnegri-ubaes.box.com%2Fs%2Fycxtnffruqg2kxke4dnh5vez243bhdxh&viewContext=inline	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2Zahh&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJuk&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZC8b&sid=z5Pk-iNyt0hd5jCcAC5e	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZfJR&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZaUl&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZcH7&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZB0b	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZPPk&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=websocket&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZC3T&sid=z5Pk-iNyt0hd5jCcAC5e	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZT2M&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZfDR&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://client-log.box.com/analytics-events/	false		high
http://https://notes.services.box.com/ep/pad/diagnosticInfo	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZC3X&sid=z5Pk-iNyt0hd5jCcAC5e	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZMuN&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=websocket&sid=z5Pk-iNyt0hd5jCcAC5e	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZIUy&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZE3r&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZLrA&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZIAI&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZB-j	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJjl&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZF_4&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZPPp&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZL2u&sid=bafhQb8Iuy6TyutvAC5k	false		high

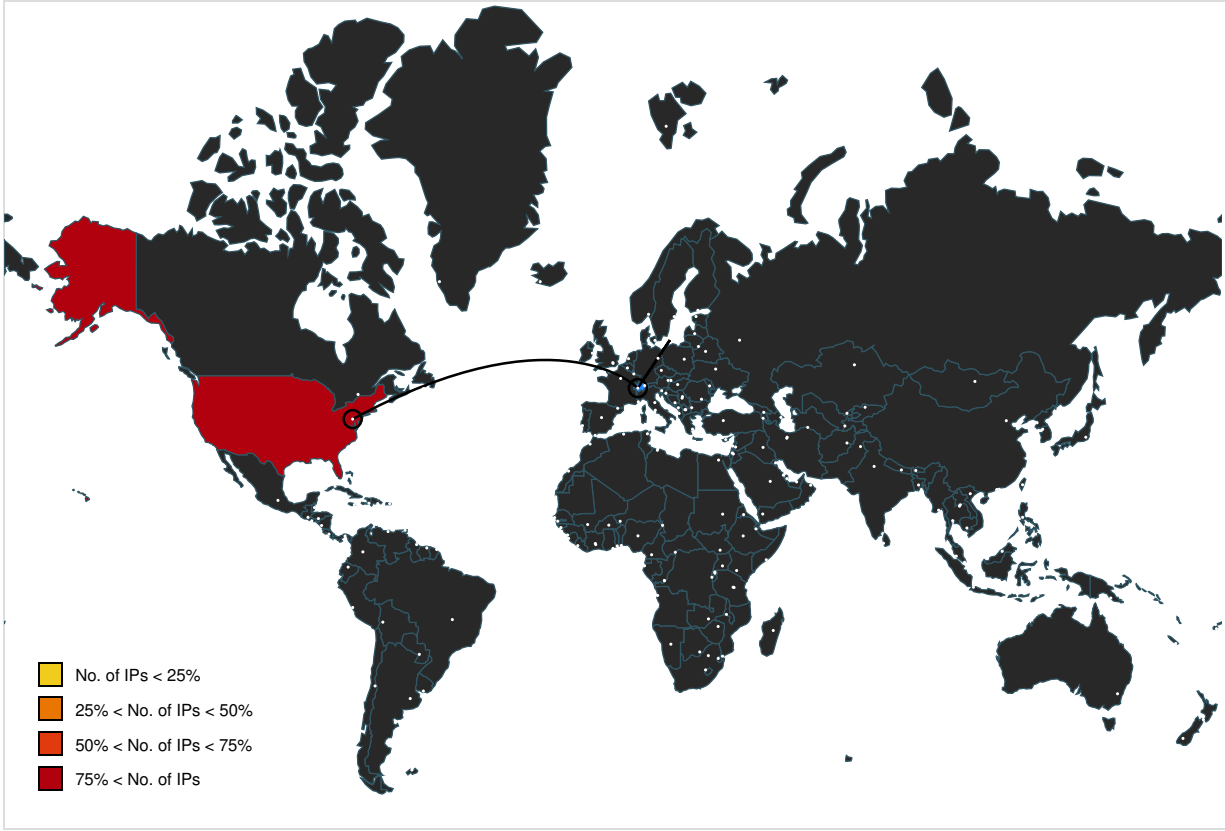
Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZCZ4&sid=z5Pk-iNyt0hd5jCcAC5e	false		high
http://https://notes.services.box.com/p/note?fileId=1169500312889&hostname=nnegri-ubaes.app.box.com&sharedLink=https://nnegri-ubaes.box.com/s/93wior2d16y21cmgyk3biklfy5s0q10w	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZCYs&sid=z5Pk-iNyt0hd5jCcAC5e	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZIsW&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://portal.microsoftonline.com/Prefetch/Prefetch.aspx	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZEp6&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZMnv&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/app_init?authCode=&fileId=1169500312889&sharedLink=https%3A%2F%2Fnnegri-ubaes.box.com%2Fs%2F93wior2d16y21cmgyk3biklfy5s0q10w&listId=inbox&_=1679374985056	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZIhy&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZK3M&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZDcI&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZIAc&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/p/note?fileId=1169500312889&sharedLink=https%3A%2F%2Fnnegri-ubaes.box.com%2Fs%2F93wior2d16y21cmgyk3biklfy5s0q10w&hostname=nnegri-ubaes.app.box.com&subdomain=nnegri-ubaes	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZDkI&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://capitaltltleandescrow.net/?oxhv	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZZdV&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZFOL&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZYU9&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZE11&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/app_init?authCode=&fileId=1169500312889&sharedLink=https%3A%2F%2Fnnegri-ubaes.box.com%2Fs%2F93wior2d16y21cmgyk3biklfy5s0q10w&listId=inbox&_=1679374988977	false		high
http://https://account.live.com/password/reset?wreply=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQQIARAA42Kw0skoKSkottLXL8gvKknM0cvNTC7KL85PK8nPy8nMS9VLzs_Vyy9Kz0wBsYqEuARMK_r-KN2d7bnloGnZ5W3H56xiVCZshP4FRsYXjly3mAT9i9I9U8KL3VJTUosSSzLz8y6wCLxi4TFgtuLg4BJgkGBQYPjBwrIlFWhTr17-q7zFa317o6PsI2MTGU6x6heXeaRaZgXl-hh4uPu4uBmWGrtlZLommbo6FoX7O3n7-YWFhboZZmVFuKfbGlsZTmATmsDGdIqN4QMbYwc7wyx2hgOcjAd4GX7wTVzz-fHLDafeegAA0&mkt=en-US	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2Ze2U&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZcGv&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://capitaltltleandescrow.net/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://https://notes.services.box.com/clientSocketConnectionInfo?fileId=1169500312889&_=1679374988978	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJz2&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJ4h&sid=bafhQb8luy6TyutvAC5k	false		high
http://https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZX8u&sid=bafhQb8luy6TyutvAC5k	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZFOK&sid=bafhQb8Iuy6TyutvAC5k	false		high
http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZKel&sid=bafhQb8Iuy6TyutvAC5k	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mbostock/d3/blob/master/src/format/requote.js	chromecache_307.1.dr	false		high
http://angular-ui.github.io/bootstrap/	chromecache_307.1.dr	false	• URL Reputation: safe	unknown
http://opensource.org/licenses/mit-license.php)	chromecache_224.1.dr	false		high
http://www.json.org/json2.js	chromecache_224.1.dr	false		high
http://getbootstrap.com)	chromecache_293.1.dr	false	• Avira URL Cloud: safe	low
http://https://openjsf.org/	chromecache_307.1.dr	false	• URL Reputation: safe	unknown
http://github.com/jquery/globalize	chromecache_203.1.dr	false		high
http://https://www.onenote.com	chromecache_195.1.dr	false		high
http://underscorejs.org/LICENSE	chromecache_307.1.dr	false		high
http://www.opensource.org/licenses/mit-license.php)	chromecache_224.1.dr	false		high
http://www.opensource.org/licenses/MIT	chromecache_293.1.dr, chromecache_307.1.dr	false		high
http://https://nnegri-ubaes.box.com/s/93wior2d16y21cmgyk3biklfy5s0q10w	chromecache_315.1.dr, chromecache_314.1.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	chromecache_293.1.dr	false		high
http://https://nnegri-ubaes.box.com/s/ycxtnffruqg2kxke4dnh5vez243bhdxh	chromecache_321.1.dr, chromecache_247.1.dr	false		high
http://github.com/angular-ui/ui-select	chromecache_293.1.dr	false		high
http://https://npms.io/search?q=ponyfill.	chromecache_307.1.dr	false		high
http://https://github.com/angular/angular.js/pull/10764	chromecache_307.1.dr	false		high
http://angular-ui.github.com/	chromecache_307.1.dr	false		high
http://https://login.windows-ppe.net	chromecache_320.1.dr, chromecache_357.1.dr	false		high
http://https://github.com/mgonto/angular-wizard	chromecache_307.1.dr	false		high
http://api.jquery.com/offset/	chromecache_307.1.dr	false		high
http://https://login.microsoftonline.com	chromecache_320.1.dr, chromecache_357.1.dr	false		high
http://angularjs.org	chromecache_286.1.dr	false		high
http://placekitten.com/150/150	chromecache_307.1.dr	false		high
http://placekitten.com/100/150	chromecache_307.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.112.186.144	nnegri-ubaes.app.box.com	United States		33011	BOXNETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
23.227.196.212	capitaltltleandescrow.net	United States		29802	HVC-ASUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
44.197.221.236	auth.split.io	United States		14618	AMAZON-AESUS	false
13.107.237.60	part-0032.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
18.165.183.9	dz87sht31vgqa.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
52.98.241.162	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830976
Start date and time:	2023-03-20 22:02:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w

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:	14
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:	mal68.phis.win@33/186@25/13
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://capitaltltleandescrow.net/?oxhv

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files 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, 172.217.168.74, 142.250.203.106, 151.101.3.9, 151.101.67.9, 151.101.131.9, 151.101.195.9, 23.10.249.185, 23.10.249.144, 40.126.32.75, 20.190.160.15, 20.190.160.12, 40.126.32.73, 40.126.32.132, 20.190.160.21, 40.126.32.137, 20.190.160.13, 23.54.112.217, 52.109.88.54, 184.86.103.152, 184.86.103.132, 13.107.6.156, 13.107.42.22, 95.100.53.90, 20.189.173.3
- Excluded domains from analysis (whitelisted): e13678.dscb.akamaiedge.net, clientservices.googleapis.com, browser.events.data.trafficmanager.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, login.live.com, update.googleapis.com, acctcdnvzeuno.azureedge.net, acctcdnvzeuno.ec.azureedge.net, e40491.dscg.akamaiedge.net, fs.microsoft.com, acctcdnmsftuswe2.azureedge.net, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, aadcdn.msauth.net, edgedl.me.gvt1.com, nel.measure.office.net.edgesuite.net, res-prod.trafficmanager.net, owamail.public.cdn.office.net.edgekey.net, aadcdnoriginwus2.afd.azureedge.net, owamail.public.cdn.office.net.edgekey.net.globalredir.akadns.net, account.msa.msidentity.com, privacy.microsoft.com.edgekey.net, www.tm.lg.prod.aadmsa.trafficmanager.net, home-office365-com.b-0004.b-msedge.net, a1894.dscb.akamai.net, acctcdn.msauth.net, acctcdn.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, prda.aadg.
- 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: 194

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	5.272684829017149
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8DHgWdzRiAU2uvxV1GgDplw05g6n:MMHdVBMHgWdzR05900+6
MD5:	A3003BF277115CB3E6E8A9097D59565D
SHA1:	517DFA0651BA5EFA8A8F607EAF1D9E4CE862F9C8
SHA-256:	101CF10E4A1188391D37233B95915DF5E346888D5BAEBCE71E1ED5F3CDB53C99
SHA-512:	C03B2107FA9251EB24FB6823B05A374CDA8214BF9D0D16C9B79B483CF0D0745479D40A4495BEC5726BE90A16A004AFDB02F0E08F582E73F7FC01178B820382D
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/Images/list_bullet_5x5.gif
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>OutOfRangeInput</Code><Message>One of the request inputs is out of range..RequestId:cf353636-d01e-001f-216f-5b4c93000000.Time:2023-03-20T21:03:34.0652438Z</Message></Error>

Chrome Cache Entry: 195

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65447)
Category:	downloaded
Size (bytes):	1289358
Entropy (8bit):	5.371176117612624
Encrypted:	false
SSDEEP:	24576:xD0TSqaj7h9pHCKaLRUku4OdiXi6SR0iFnTghQo4kpVjWp4jrRBouNHunz6gznlp:USqaj7h9pHCKaLRUku4OdiXi6SR0iFnr
MD5:	B5146DE5F6ED29229B543C2780047B21
SHA1:	0CED2F822087BE4117DDD7E3A1B5A67F2B621B9A
SHA-256:	D8F528D7631D732E136A41AA3F58AB1163F4BF937E76BF7DAC710CD79692A287
SHA-512:	2AC5F108B6BBDEE5566ADC01A9097C10795AF9D3A10466BEFFBFAB85D9EEC2AFC6661069AB510409FE7C6877EFEAD213128B94F1154E1D5B49DDD9C569E5A34F
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/officehub/bundles/app-bundle-9b368a4cedcd3787b600.js
Preview:	/*! For license information please see app-bundle-9b368a4cedcd3787b600.js.LICENSE.txt */.!function(e){function t(t){for(var i,r,s=t[0],c=t[1],u=t[2],d=t[3]||[],p=0,h=[];p<s.length;p++)r=s[p],Object.prototype.hasOwnProperty.call(o,r)&&o[r]&&h.push(o[r][0]),o[r]=0;for(i in c)Object.prototype.hasOwnProperty.call(c,i)&&(e[i]=c[i]);for(f&&f(t),l.push.apply(l,d);h.length;)h.shift()();return a.push.apply(a,u||[]),n()}function n(){for(var e,t=0;t<a.length;t++){for(var n=a[t],i=!0,r=1;r<n.length;r++)0!==o[n[r]]&&(i=!1);i&&(a.splice(t--,1),e=c(c.s=n[0]))}return 0===a.length&&(l.forEach((function(e){if(void 0===o[e]){o[e]=null;var t=document.createElement("link");t.crossOrigin="anonymous",c.nc&&t.setAttribute("nonce",c.nc),t.rel="prefetch",t.as="script",t.href=s(e),document.head.appendChild(t)}})),l.length=0),e}var i={},r={92:0},o={92:0},a=[],l=[];function s(e){return c.p+""+({9:"officehome-async-styles",21:"vendors~action-context-menu-rc~app-gallery-rc~app-host-component~appbar~catchupflyout~cc~

Chrome Cache Entry: 196

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:lpQ9KDQmYm1j7xS7kmObTyQW620xdxClmqCzP/XDKFjy9iwjn7nQNOSfclLQD2mV:lpQ9KDQmYm1j7xS7kmObTyQW620xdxCF
MD5:	B5307E4A0D56B62E41600E1296BF75AA
SHA1:	76B57440EFC1A382989E8BED80379D2C00FCA64B
SHA-256:	DEF6F66252A9F848DFBE00904DF6D26A4215051EC39C7CB361AAACDC2BAAD889

SHA-512:	F028F5DDFB6405838AA5DC50BD8E52F120173D4A6DF9F2197AE5ECD6BF0B1246E6B186A0453AA31D45A5CE7FFF486CD578FC6A459A48A321EA97CF2596CD70 35
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: 197	
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:	9AA8B1FEFE162CC6F8C51FE06BE53DE2FF86E9953BB3B58B7821FDABF7A4062C69621FF65E2A666927BA2C28A87D81B03C275D8A4415E5A0E6E32EB7245022 C8
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: 198	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	183
Entropy (8bit):	4.91551109797976
Encrypted:	false
SSDEEP:	3:4ovtrKIvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLtjYWRZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EGWeiWoTZHTV
MD5:	6895548091748CFCF47BE6560216595A
SHA1:	A721FE8074CF3BCEB53A810AA9C4C20B7E326A15
SHA-256:	D320CA79C98D26B2847C2EAABBDDB45B932A681603213D3C44DD7491E6CAE443
SHA-512:	6970E70857CAF2A3189A26C36995FE4A61B9EC613C0F37307B2B4AE5DC14F9EB3295281D3CE59146999ADCC9BEEA4F5A3E0645A98CA1D07DD123A255FB6383 2
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZE3r&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":false,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 199	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.258782286369088
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH1q4vwV1s0lZLH8g6n:MMHdVBKW/UT4oKJHx6
MD5:	72CB7B223975D63591E3397735766D58

SHA1:	EC6865AC5093F9D7D5CE824754D8E1848FA8F859
SHA-256:	C2985735B5BDE9DA6A3DE1BE729BADB616CC03F520316AF054360D537F87ADA2
SHA-512:	6B9745842AA8C379618D09C69E3E9531C0EFF4BA77956FBE456A40D72328584E6CDCE7D7432844E8AAA6CDF0243A3DA0D994C0E38DA3B4F9EA135EE049E7F82
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/images/scrollbar/arrow_staticup_16.png
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:b6e81507-701e-0046-456f-5bfe46000000.Time:2023-03-20T21:03:57.6717898Z</Message></Error>

Chrome Cache Entry: 200	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (7808), with no line terminators
Category:	downloaded
Size (bytes):	7808
Entropy (8bit):	5.229365087117069
Encrypted:	false
SSDEEP:	96:L+qs9f6jGaJDM2j/jHHe0Oy6qkmYdcCXiwLPzwL5AcP0F0mqDY3cpS7Z:CCGaG8jrjkmYdcBwLPz4OVvqsMpSd
MD5:	CFAC4D37EBEE0DEB9CA7FF514C67910B
SHA1:	DA0A3FC895086FC6094B24811EC6E494ACACC4C8
SHA-256:	6FEDAE5107F342161BA5B8DC77D5D20A77FEEC58A4417A4CB14C8BAA883D157E
SHA-512:	40DB53C62062B2527DEC3594A669F3A4B32A44F5DF4C0141281EABBCDD0518FA52414C6A862BB1E7A0932C1E9BDB3F13EC5A4BE74C53ADBA73CAC78A460A753E
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/webcontrols/js/gridview.js
Preview:	var GridViewManager={};GridViewManager._gridViewInstanceIds=[],GridViewManager._gridViewInstances=[],GridViewManager.CreateGridViewInstance=function(n,t,i){var r=n.replace(/_Grid_ListViewUpdatePanel$/i,""),u,f;return GridViewManager._gridViewInstanceIds[r]?null:(u=new GridViewInstance(r,t,i),f=GridViewManager._gridViewInstances.length,GridViewManager._gridViewInstances[f]=u,GridViewManager._gridViewInstanceIds[r]=f,u)},GridViewManager.GetGridViewInstanceByID=function(n){var t=GridViewManager._gridViewInstanceIds[n];return GridViewManager._gridViewInstances[t]},GridViewManager.GetGridViewInstance=function(n){var t=null,i,r,u;if(n){for(i=/(_Grid_ListViewUpdatePanel)|(_LayoutUpdatePanel)$/i;n&&(!n.id||!n.id.match(i));)n=n.parentElement;n&&n.id&&(r=n.id.replace(i,""),u=GridViewManager._gridViewInstanceIds[r],t=GridViewManager._gridViewInstances[u])}else t=GridViewManager._gridViewInstances[0];return t},GridViewManager.LoadInit=function(){var t,n;for(Sys.Application.remove_load(GridViewMana

Chrome Cache Entry: 201	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.278623785808387
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH1hZErrclZLx3o8g6n:MMHdVBKW/UTL6ux3+6
MD5:	6C98AB3789DC0E37018A9AA716BAC206
SHA1:	89687BE73880A1C6FE5C9890BF524A321E654ECB
SHA-256:	3B20371B3933AE3C40B73DE6823974A43294367A74483AE4EA35FA1F7F839730
SHA-512:	05831F5FEAE26FD9409C952EAB77B1E0260F438F8592386F927F468CC5E95996346ADF44393ED7C41146069D45006CCBCB0AB6D1CAA5090B56E2F9340098DB14
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/images/servicestatus.png
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:905a35b8-601e-004a-7c6f-5b694e000000.Time:2023-03-20T21:03:57.4538478Z</Message></Error>

Chrome Cache Entry: 202	
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: 203

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (59783), with CRLF line terminators
Category:	downloaded
Size (bytes):	663451
Entropy (8bit):	5.3635307555313165
Encrypted:	false
SSDEEP:	12288:YhqblwQ9eTw/suNyIzaJS/pWYawUWufSxwDr2o/5YP1B:Yhqblt9e8/sMzaJS/pWYawUWufSxwDrW
MD5:	761CE9E68C8D14F49B8BF1A0257B69D6
SHA1:	8CF5D714D35EFFA54F3686065CB62CCE028E2C77
SHA-256:	BEAA65AD34340E61E9E701458E2CCFF8F9073FDEBBC3593A2C7EC8AFEACB69C1
SHA-512:	CEC948666FBA0F56D3DA27A931033C3A581C9C00FEC4D3DDCF41324525B5B5321AE3AB89581ECC7F497DE85EF684AB277C8A2DB393D526416CEB76C91A1B9 63
Malicious:	false
Reputation:	low
URL:	http://https://r4.res.office365.com/owa/prem/15.20.6178.37/scripts/boot.worldwide.0.mouse.js
Preview:	.window.scriptsLoaded = window.scriptsLoaded || {}; window.scriptProcessStart = window.scriptProcessStart || {}; window.scriptProcessStart['boot.worldwide.0.mouse.js'] = (new Date()).getTime();../* Empty file */;Function.__typeName="Function";Function.__class=!0;Function.createCallback=function(n,t){return function(){var r=arguments.length;if(r>0){for(var u=[],i=0;i<r;i++)u[i]=arguments[i];u[r]=t;return n.apply(this,u)}return n.call(this,t)}};Function.prototype.bind=Function.prototype.bind||function(n){if(typeof this!="function")throw new TypeError("bind(): we can only bind to functions");var u=Array.prototype.slice.call(arguments,1),r=this,t=function(){},i=function(){return r.apply(this instanceof t?this:n,u.concat(Array.prototype.slice.call(arguments)))};this.prototype&&(t.prototype=this.prototype);i.prototype=new t;return i};Function.createDelegate=function(n,t){return function(){return t.apply(n,arguments)}};Function.emptyFunction=Function.emptyMethod=function(){};Error.__typeNam

Chrome Cache Entry: 204

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (4787), with no line terminators
Category:	downloaded
Size (bytes):	4787
Entropy (8bit):	5.3136178165749515
Encrypted:	false
SSDEEP:	96:5iBUcCRgqJY+ebZFBfquEiwQYGQwnCSo3DijVxlJz/odkFVMhMY7PHYh+O8C:5i/PquEiwQ/QJzDeVnN/odkbMhMY7PHI
MD5:	D4A9893F26D6C6BA6370D1AA877D9530
SHA1:	616E7478F40C2EE6DDE03C7D6AFA35265211EDBD
SHA-256:	329E33E61952A1445BF79F6D073FF443339AA13E6338C568D20A3015C0E7BF9E
SHA-512:	9870638699DD51E0EEF34BCE532E24B585FE02E3BB52AE62F0389E97904EE04A12646D24041F277718938A1EA3AF257BDB6D136514B97AB0790FF1E9C1F40820
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/netperf.js
Preview:	function NetPerf(){function c(r){var u,l=[],p=["i":30000,"v":3'],o,a,y,s,h,v,c;if(l.push(p),u=[],r=='u')e?(u.push('0'),u.push('1')):(u.push('1'),u.push('0'));else if(r=='l')u.push('0'),u.push('0'),e=!0;else return;for(o=null,y=f.length,s=0;s<y;s++)h=window.performance.timing[f[s]],o==null?o=h:(a=h>0?h-o:-1,u.push(a));if(u.push(""+n.encodeJsonStringLiteral(document.URL)+""),u.push(n.edgeInfo.isEdge?"1":"0"),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.ds)+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.f.toString())+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.cid)+""),v=[],n.edgeInfo.prop)for(c in n.edgeInfo.prop)n.edgeInfo.prop.hasOwnProperty(c)&&v.push(c+'='+n.edgeInfo.prop[c]);u.push(""+n.encodeJsonStringLiteral(v.join(t))+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.wl)+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.tid)+""),u.push(""+n.encodeJsonStringLiteral(n.edgeInfo.ipv)+""),l.push('"f":['+u.join(t)+']'),i.push('{'+l.join(t)+'}')}function

Chrome Cache Entry: 205

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	215
Entropy (8bit):	5.299607513760371
Encrypted:	false

SSDEEP:	6:JiMVBdgqZjZWtMfgRTH1952c6HG//VclXN05g6n:MMHdVBZWyUTH5o0+6
MD5:	270F19B2DE94431A6D29D67889364A0B
SHA1:	C1E4DB76D2F578D9CA347567D6B392822C0DA98D
SHA-256:	30CBA27EC1404B95FFD2F4E71D5566ECA92E0B2A07B4B98467C091942DD577AB
SHA-512:	09F2BD062F595F63C326F8A2D0FCCB34A54DDEFBFFEF8E7889486EB15B667FCFC8D0C68EE52C5B38D9A2B52379350CD4F5968E80E0E8DCCE8FFA3AF9B48CC A52
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/searchbox.js
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>BlobNotFound</Code><Message>The specified blob does not exist..RequestId:426e293b-d01e-0012-686f-5 bb111000000.Time:2023-03-20T21:03:56.4074088Z</Message></Error>

Chrome Cache Entry: 206	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 1592
Category:	downloaded
Size (bytes):	621
Entropy (8bit):	7.673946009263606
Encrypted:	false
SSDEEP:	12:Xp7fmqfW/e4YC2L0E5DZLB62y/+6lbPa1Gotq8mdd2Xmy2QLBwxD+QkCfBJ:Xp6qf2SCk3LBpy/rtPa1GKq8mOX5jLcD
MD5:	4761405717E938D7E7400BB15715DB1E
SHA1:	76FED7C229D353A27DB3257F5927C1EAF0AB8DE9
SHA-256:	F7ED91A1DAB5BB2802A7A3B3890DF4777588CCBE04903260FBA83E6E64C90DDF
SHA-512:	E8DAC6F81EB4EBA2722E9F34DAF9B99548E5C40CCA93791FBEDA3DEBD8D6E401975FC1A75986C0E7262AFA1B9D1475E1008A89B92C8A7BEC84D8A917F221B 4A2
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg
Preview:	.....}UMo"1..+.....G; .8l...M..$.U.AW.....UaX..`'.=.....\|..z3...Ms>..Y...QB..W..y..6.....?.....L.W=m....=..w.)...nw...a.z.....#.y.j...m...P...#...6....6.u.u...OF.V..07b..\...s .f..U..N..B...>.d.-z..x.2..Lr.Rr)....JF.z.;Lh.....q.2.A....[.&".S..:.....]........#k.U#57V..k5.tdM.j.9.FMQ2..H:.~op..H.....hQ.#...r[.T.$.@.....j.xc.x0..I.B:#{iP1.e'..S4.:...mN.4)<W.A.) .g.+..PZ&.$.#.6v.+.!...x*...}..._...d...#.Cb..(..^k..h!..7.dx.WHB.....(.6g.7.Wwt.I<.....o.;....Oi$}f.6.....:P..!<5.(.p.e.%et.)w8LA.l9r..n.....?.F.DrK...H....0F...{.,.....{E..".....*...x.@..? u...../....8...

Chrome Cache Entry: 207	
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.....nnnooyyyvvvllppp.....~~ ~}}}|||.....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: 208	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	5.054890155232238
Encrypted:	false

SSDEEP:	12:TEwlu2e3E5VvNGwlu2mX3EArWFJwlu2e3EavNGwlu2mX3EArWF2:TEiupi0iujzqFJiupF0iujzqF2
MD5:	E35AA23ECEE77EBCFFF93487F4544755
SHA1:	BF3F97F2FCA7A08C9E7CFBA8438143DC0017BCCB
SHA-256:	137A3D46ACFAD27AEFAC5EF42684608AE871D90DC5E22211FA1D9CF96F6B1FF2
SHA-512:	81073CD9DADC19E79C57E1B64DDF7EC33F78C8EF816967AE86EA4B046C0738CD66D4A807B2E4FFA6DB4A0E8B582FE669E2058499C1804D08586803580786FB4B
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZMnv&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":false,"userId":"2","name":null,"hasCustomAvatar":false}]}}].42["message",{"component":"PM_DOC","type":"USER_CURSOR_CHANGED","response":{"error":null,"data":{"userId":"24404463343","userPosition":{"head":198},"docVersion":10,"docOrSelHasChanged":false}}}].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":"USER_CURSOR_CHANGED","response":{"error":null,"data":{"userId":"24404463343","userPosition":{"head":198},"docVersion":10,"docOrSelHasChanged":false}}}]

Chrome Cache Entry: 209

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.066130335315081
Encrypted:	false
SSDEEP:	6:tI9mc4slz2lWjVRqtmd9QA0ZcTKhqnR40Y:t44lWjVRqtnA0Zcq6R40Y
MD5:	2974998C6B3220B65AA137F4B08F57F8
SHA1:	F4F08DA689179DE68EE40CD12ECDCC5AC54B3979
SHA-256:	96D52BD03E244A44931A541A807067792D638DD29EC14A87A78F2BE85D12D19A
SHA-512:	6B4F2439CA99109A7C97828E5972A8E7C7FCA3745B2FB4738EBD9329A99234A8CD3BC4C0C48B5BAA917D4BAA64CDAEB5D74456DEFDDDA3E07FAA803283BE0287
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="36" height="36" viewBox="0 0 36 36"><title>assets</title><path d="M18,22.484l-8-8,.969-.968L18,20.547l7.031-7.031.969.968-8,8Z"/><rect width="36" height="36" fill="none"/></svg>

Chrome Cache Entry: 210

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/ChRDaHJvbWUvMTA0LjAuNTExMi44MRJBCUyNkHQka1nUEgUNSoWeUhIFDUqFnIISBQ0G7bv_EgUNBu27_xIFDUqFnIISBQ0G7bv_EgUNBu27_xIFDUqFnIISQQl5IRIOPvT4jxIFDUqFnIISBQ1KhZ5SEgUNBu27_xIFDQbtu_8SBQ1KhZ5SEgUNBu27_xIFDQbtu_8SBQ1KhZ5S?alt=proto
Preview:	CkgKBw1KhZ5SGgAKBw1KhZ5SGgAKBw0G7bv/GgAKBw0G7bv/GgAKBw1KhZ5SGgAKBw0G7bv/GgAKBw0G7bv/GgAKBw1KhZ5SGgAKSAoHDUqFnIIaAAoHDUqFnIIaAAoHDQbtu/8aAAoHDQbtu/8aAAoHDUqFnIIaAAoHDQbtu/8aAAoHDUqFnIIaAA==

Chrome Cache Entry: 211

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96

SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0 1
Malicious:	false
Reputation:	low
URL:	http:// https://acctcdn.msauth.net/images/favicon.ico?v=2
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(...................(....................................."P......................................"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""""""""

Chrome Cache Entry: 212

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	194
Entropy (8bit):	5.014114983792889
Encrypted:	false
SSDEEP:	3:4ovtrKIvFCm/JfQ2gfqKPv3ULWAlHxAQWAXc13TwJQ3UFExGBdxPIs2stEtAp6Vn:4ovMwl/m2mX3EADyG3GX1dU
MD5:	F370E30DC1DAB486C60B724AF0F410A9
SHA1:	D4370031DA06A97C28B6ED586F86CF501E856A3A
SHA-256:	D87F086251B8BC81B39E311BBAEC832AA5E56FF24738A59BF0EBA2EE3EAA1231
SHA-512:	2026BA907A22EF38889F6C5451C8E792A58E0465A7387F0080489712764A651AE00143A2E502F2351306DDF6B28767507594CA37E12634FFA050E1852B9312BD
Malicious:	false
Reputation:	low
URL:	http:// https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZZZR&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USER_CURSOR_CHANGED","response":{"error":null,"data":{"userId":"24404463343","userPosition":{"head":198},"docVersion":10,"docOrSelHasChanged":false}}}]

Chrome Cache Entry: 213

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	dropped
Size (bytes):	2672
Entropy (8bit):	6.640973516071413
Encrypted:	false
SSDEEP:	48:ZaOdwduTYPpS9pZy9vDNi1miicsvrJkafMiS+MGQ09DU/X9/4Xp6m5Z9SQcq:4CIuTYPpSTc9vcPZX9/2gzQ/
MD5:	166DE53471265253AB3A456DEFE6DA23
SHA1:	17C6DF4D7CCF1FA2C9EFD716FBAE0FC2C71C8D6D
SHA-256:	A46201581A7C7C667FD42787CD1E9ADF2F6BF809EFB7596E61A03E8DBA9ADA13
SHA-512:	80978C1D262BC225A8BA1758DF546E27B5BE8D84CBCF7E6044910E5E05E04AFFEFEC3C0DA0818145EB8A917E1A8D90F4BAC833B64A1F6DE97AD3D5FC80A02 308
Malicious:	false
Reputation:	low
Preview:	GIF89a`............!..NETSCAPE2.0.....!.......,....`.....6......P.l.......H....I..:qJ......k....`BY..L*..&...!.......,....0.............<....[.\K8j.tr.g..!.......,....3...........^;.*..\UK.]\.%.V.c...!.......,....7........`....lo...[.a..*Rw~i...!.......,....;........h.....l.G-.[K.,_XA]..'g..!.......,....?........i.....g....Z.}..)..u...F..!.......,....C...............P.,nt^.i....Xq...i..!.......,....F...........{^b....n.y..i...\C.-...!.......,....H..............R...o....h.xV!.z#...!.......,"...L.............r.jY..w~aP(.......[i...!.......,(...N.............r....w.aP.j.'.)Y..S..!.......,....H.........`......hew..9`.%z.xVeS..!.......,5...A.........`...\m.Vmtzw.}.d.%...Q..!.......,9...=.........h......3S..s.-W8m...Q..!.......,A...5.........h.....N...:..!..U..!.......,H.............h....M.x...f.i.4..!.......,O...'.........i...tp......(..!.......,X.............j...@.x....!.......,]............j..L..3em..!.......,e.............`......!.......,n..............{i..!..

Chrome Cache Entry: 214

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	813
Entropy (8bit):	0.3777162536454919
Encrypted:	false
SSDEEP:	3:CUDu//tylaJqAlTlmhy:EX7JqAcy
MD5:	DBC2B30ECD3CE2A7A8965E5B0A569DFF

SHA1:	C32D2FFDBF66B5582C8C184E0C0B436048292807
SHA-256:	9397D5506D9BB44184A4BD44001382209441BD80D8C5FB4F3DFFDB1F966B7995
SHA-512:	496E07788F07A4F31E690E67367086FBAA934CFAEF0256F669B395ADF0EBF8C677D3775BEAB50F5100D178B67F51F5F2AAA7CE8B89EC5B93CAE6F3B2C21BFD6F
Malicious:	false
Reputation:	low
URL:	"https://portal.microsoftonline.com/pp.l?CID=ce5ec8bcaaf4406a94cd2be1e488444a&pageId=Prefetch.aspx&d={B:{S:%27L%27,LT:4228,UT:-1,MT:-1},A:{ET:-1,OT:20,DT:160,CT:285,RT:370,ST:375,MT:-1,LT:4640},C:{LT:1679375037696}}"
Preview:	GIF89a..... ....I..... .....;

Chrome Cache Entry: 215

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	215
Entropy (8bit):	5.2777184474807
Encrypted:	false
SSDEEP:	6:JiMVBdgqZjZWtMfgRTH11q6A/fuhlJlTc8o8g6n:MMHdVBZWyUTT0/mdix6
MD5:	64BCBD7C0FE175D0574351712EF40049
SHA1:	97B6D0887D83B77DD651E3C6D7403BB4DF3E3F34
SHA-256:	A23600F12D5E5FDC2E4E872EEAB139647DF104C7A432BDE3B9161496D183DA5B
SHA-512:	7A44A945F674CDA8881072CD3AF1CB5DD505933A00D1E2AB6D980437A58647FB26546FAEE9487B4A0F86886DBCCA61653A1192653FD94215BF242AA62015EE7
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/assistancepanel.js
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>BlobNotFound</Code><Message>The specified blob does not exist..RequestId:18030601-b01e-0066-2d6f-5b85e1000000.Time:2023-03-20T21:03:34.3273692Z</Message></Error>

Chrome Cache Entry: 216

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:JEd0lY9YbGvf6ZAX2pLKOF7jJfyNRLhqcGeSi2475rwNLj5LMF1AM2QMhKZl8fh: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: 217

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D

SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
URL:	http://https://account.live.com/Resources/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

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):	32
Entropy (8bit):	4.375
Encrypted:	false
SSDEEP:	3:4HvpoEmTH6t+Y:4PITH++Y
MD5:	8E17F1BD7D65C3C7D8906AEAF7B2EC94
SHA1:	2C9B4306D9888952E64D888C1FDED11933404405
SHA-256:	1B01C622D0EDB317B4B6A7DDD8F79BC49641112451F82943C115805DDDE36A91
SHA-512:	3B50D37F37118C5A4DBA9F2F87AB8C2AE5E0DEF64A2D1DD813AFA7D6007AA6FD0DEED618E42CDF1A1A2F03CDB7D5132F58DB556AF475AEEB1C833ACBB620 58AD
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZDcK&sid=bafhQb8Iuy6TyutvAC5k
Preview:	40{"sid":"fP5-O_JCvyhs_IhTAC5l"}

Chrome Cache Entry: 219

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (575)
Category:	downloaded
Size (bytes):	2721
Entropy (8bit):	5.084992914599531
Encrypted:	false
SSDEEP:	48:VgG0V3B1c3PAky2otyX8v9M6xJoaAdarOGsOkbtzmymwYLx+CgF:VgPV3Bu3auXwM6voa24ktmyhYdw
MD5:	C862B2F23031F112F66CBAA6045D3ADF
SHA1:	7451E792AD5F97A751CA6FF799B692DD59F0D405
SHA-256:	978468706EFA64F5EF4681FC0136D0FC1AB0F9BEC93CE878B873FDB7DE968EEA
SHA-512:	A380FF9585C8FB427BEB90824EF2232AB0C214AB1EF9454C0B742EBB1020D628C6048534E970580452AC8CE00F984277688B43EEFE4A187AAF4274BD760B8F24
Malicious:	false
Reputation:	low
URL:	http://https://acctcdn.msauth.net/bootstrapcomponentshim_yGKy8jAx8RL2bLqmBF063w2.js?v=1
Preview:	!function(){function e(e){var t;return"function"==typeof Event?t=new Event(e):(t=document.createEvent("Event"),t.initEvent(e,!0,!0)),t}function t(e){return e.keyCode||e.which}function n(n){n&&3===t(n)||($PageHelper.byClassName(r).remove(),$PageHelper.queryAll(o).each(function(t,a){var r=$PageHelper.get(a),o=r.parent();o.hasClass("open")&&(n&&"click"===n.type&&/input\|textarea/i.test(n.target.tagName)&&o[0].contains(n.target)\|\|(o.trigger(n=e("hide.bs.dropdown")),n.defaultPrevented\|\|(r.attr("aria-expanded","false"),o.removeClass("open").trigger(e("hidden.bs.dropdown"))))}))}function a(){$PageHelper.queryAll(o).each(function(e,t){t._msaDataCache=t._msaDataCache||{},t._msaDataCache["bs.dropdown"]=new i(t)})}var r=".dropdown-backdrop",o='[data-toggle="dropdown"]',i=function(){function a(e){var t=this;this.element=e,$PageHelper.get(this.element).on("click.bs.dropdown",function(e){return t.toggle(e)}).on("keydown.bs.dropdown",function(e){return t.keydown(e)}),$PageHelper.byClassName("dropdow

Chrome Cache Entry: 220

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):	320174
Entropy (8bit):	5.9970337158865785
Encrypted:	false
SSDEEP:	6144:lV5xjzkWx05Da2N5q40OBQpJF2UfqPVV5qnobZnCIx52K+g6jG:j5xPkWx2227qe2pJFRfqPVVQnobZ1x5H

MD5:	02130E4F0DC9B5017D66C32F2CC32CE2
SHA1:	8898F4B4D2D2D40F9F1E898210AC30E868618C4B
SHA-256:	60150F61CAAF4C11ADFDB527A4A024AAFDA50CF24BADC98F0157643B3E750A96
SHA-512:	11300160D5442D0F7AFE224569F035AF45AEF4E1E99EFFA774B765644FCCBF68944C0C9A6D76651B2C37839A9DE69053A1C1B4CB244655EB99E2E12C70051182
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/box-image?encoding=base64&fileId=1169506039580&fileName=Box%20Notes%20Image%202023-03-20%2010.57.19.png&sharedLink=https%3A%2F%2Fnnegri-ubaes.box.com%2Fs%2Fycxtnffruqg2kxke4dnh5vez243bhdxh&viewContext=inline
Preview:	FVqMJNECTBbpLd0yM7I7lzK7siT2T+1BXZ9+Ttzptmsw+e3c0mu3kTJAFeIAmAuI8C6sjMcDPdH0zVzNzD4w6PCI80JROV6cfn5qpu5q43MTNjDmIAlPzbvnc5Wu3szePO xmYwaOlrb4LXXWB3RZvgdZfYm5fjblKW46LjXp72de3bVTl2RXnOLIq9m5TluOi4d5Py2rcoT5anWbzubsy7z+v8Dtscdp/mzKJE8xoAMmXKlClTpkyZMXKlCITpkyZMmXKlCITpkz9JT N9Ny+5b5VjLypti9cXUY5d3kcf5Lgv1MU9c+PfVa97EeWyKPVhzuyLHPPatx+U1779oC55neW4Ocpr3+ZoH9e+7cjRTL95mrKsUNvGCbdCrVvnXrIWXdtm71765GVwa+fw rvF6Duzwy4pynMmcFXCmnjwfrxcbap/l2l7UpRxXoqXmzLxDbWJT+Devfavjbm7tSwP2Zo9743KcyZwVcKaenNe+8ZP3V44Xa+2bD3tu2ru1b0fkOJM5K+AsePJuy1GPzW vflBtAN++wba993chxFk1IAegyQyFj93/MfcXu45gz9n6MOWPvx5gz9n6Mua/YfRxzxt6PMWfs/RhzX7H7OObdxp6QArDCYGeaIRbDnmH06Af2GnFr2Gse82l3sKO8noq9 Aq9nUub1WrHXiNs19kb40VfsNeLWsPPat1nsNeLWsPvKj/wOW/AifeT1ithrxK1h57Vvs9hrxK1h95Ufee1b8CK7y2uz0NltaOPRGfNefq6R1uD6ij3PCctgr8uolOU4H/ a6KPN6NvY8J3SCvQBuluNs7HlOWAY7r32bxV4XdSnHTfKjr9jroDxn5sOe54RlsPPat1nsdVHHctwLXvdljr3nB+UuAHNTl0Ecme

Chrome Cache Entry: 221

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	680
Entropy (8bit):	5.7619518976999045
Encrypted:	false
SSDEEP:	12:Y1JG3BWPRr7D2l9ctU8XlOrVTvUyOF/qAngktLQFeDIcyjhMe:Y1JG3sRr7DJtU8XvrVIRJrtLBFehMe
MD5:	50C1B0FD8755754C694DBDE23D194675
SHA1:	73FCDF016EDA48EF052D4FA8B9236C21AED7E8F7
SHA-256:	1E7B33ED0213A7DA305D280AFFAEEBD54A5E96B4A58B4A20868A14E66E481FB0
SHA-512:	98E10CD2F1449E41EE75925AF3B4792059D5CA4D13907E6C4D624CB61FAA0CE53BFD0F39681688F469E26FA852754C110C58CDB60F5D6D926B5135323537D3A
Malicious:	false
Reputation:	low
URL:	http://https://auth.split.io/api/v2/auth?users=key
Preview:	{"pushEnabled":true,"token":"eyJhbGciOiJIUzI1NiIsImtpZCI6IkRQVkE3QS44czhnaVEiLCJ0eXAiOiJKV1QifQ.eyJ4LWFibHktY2FwYWJpbGl0eSI6IntcIk9EYzFOVEE1TURRd19Nall3TnpJek56YzFNUT09X2NvbnRyb2xcIjpbXCJzdWJzY3JpYmVcIl0sXCJPRGMxTlRBNU1EUXdfTWpZd056SXpOemMxTVE9PV9teVNlZ21lbnRzXCI6W1wic3Vic2NyaWJlXCJdLFwiT0RjMU5UQTVNRFF3X01qWXdOekl6TnpjMU1RPT1fc3BsaXRzXCI6W1wic3Vic2NyaWJlXCJdLFwiY29udHJvbF9wcmlcIjpbXCJzdWJzY3JpYmVcIixcImNoYW5uZWwtbWV0YWRhdGE6cHVibGlzaGVyc1wiXSxcImNvbnRyb2xfc2VjXCI6W1wic3Vic2NyaWJlXCIsXCJqaGFubmVsLW1ldGFkYX RhOnB1Ymxpc2hlcnNcIl19IiwieC1hYmx5LWNsaWVudElkIjoiY2xpZW50SWQiLCJleHAiOjE2NzkzNDk3OTIsImlhdCI6MTY3OTM0NjE5Mn0.Xwvby8ehrHyip6YFX_Ka bqgtOyXkplaqTYvKTovqrUs","connDelay":60}

Chrome Cache Entry: 222

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	183
Entropy (8bit):	4.91551109797976
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLtjYWRZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EGWeiWoTZHTV
MD5:	6895548091748CFCF47BE6560216595A
SHA1:	A721FE8074CF3BCEB53A810AA9C4C20B7E326A15
SHA-256:	D320CA79C98D26B2847C2EAABBDDB45B932A681603213D3C44DD7491E6CAE443
SHA-512:	6970E70857CAF2A3189A26C36995FE4A61B9EC613C0F37307B2B4AE5DC14F9EB3295281D3CE59146999ADCC9BEEA4F5A3E0645A98CA1D07DD123A255FB6383 2
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZWhm&sid=bafhQb8luy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":false,"userId":"2","name": null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 223

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223

Entropy (8bit):	5.219160086861945
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH162/UgglhRrAg6n:MMHdVBKW/UTngF6
MD5:	EC84495DAA368D48A11499E941623211
SHA1:	5F9B0905DF0D311D79AA8DDB7BB4B11CAB7BF3DF
SHA-256:	A01E7CA6E21D0677BCAD5E9E3A50B17BBCFBB5C18E7D40F7314B9E2DA79425D8
SHA-512:	0527AC2DFA12FC7F70F57267E9EB1F1EBB5BF331027CA47C588041023BF66D9EECCBBE3C5A47CD50983E4F6087CE3A5B76B29705DF5E05B96506A587038961ED
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/shell/images/o365_gallatin_logo.png
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:6d592c3f-001e-0011-1a6f-5b5075000000.Time:2023-03-20T21:03:35.1178681Z</Message></Error>

Chrome Cache Entry: 224

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (6619), with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	78311
Entropy (8bit):	5.421676443255173
Encrypted:	false
SSDEEP:	1536:yOWjonYwd51CleWm3vTJhFR0aXBo1nuQvEODDRLmutNnbt:xP5Cf5/bt
MD5:	189EB673A0FD4791EE285764A0EF1763
SHA1:	13273A13087F0B15C2D9E8C72EA1CAF2E1256B07
SHA-256:	C58E92C3ABAC24575F36960372E39F10AC0E20B3C33B605F2B3D3E1498ACF025
SHA-512:	C59597872F1A972D6F2E08B51C95F1E497B4765BC468086F0AA98F8F9D31504E17349EE114D17C35BE31B2784ED3F3D4097954142E7D9A6CC75C97CC3FAA0838
Malicious:	false
Reputation:	low
URL:	http://https://acctcdn.msauth.net/knockout_old_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1
Preview:	/*!---------- START OF THIRD PARTY NOTICE ----------....This file is based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. .... * Knockout JavaScript library v3.2.0.. * (c) Steven Sanderson - http://knockoutjs.com/.. * License: MIT (http://www.opensource.org/licenses/mit-license.php)....Provided for Informational Purposes Only....MIT License ....Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the Software)

Chrome Cache Entry: 225

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 352 x 3
Category:	dropped
Size (bytes):	3620
Entropy (8bit):	6.867828878374734
Encrypted:	false
SSDEEP:	48:ZumKaT5ezv47j2/ZiRDlq16x8XvEUcg777shHdpHVGJqFd:Eal647jPDlL8XvEUcg77kVGyd
MD5:	B540A8E518037192E32C4FE58BF2DBAB
SHA1:	3047C1DB97B86F6981E0AD2F96AF40CDF43511AF
SHA-256:	8737D721808655F37B333F08A90185699E7E8B9BDAAA15CDB63C8448B426F95D
SHA-512:	E3612D9E6809EC192F6E2D035290B730871C269A267115E4A5515CADB7E6E14E3DD4290A35ABAA8D14CF1FA3924DC76E11926AC341E0F6F372E9FC5434B546E5
Malicious:	false
Reputation:	low
Preview:	GIF89a`.....iii!.....!.&Edited with ezgif.com online GIF maker.!..NETSCAPE2.0.....,...`.....6.....P.I.....H....I..:qJ.....k....`BY..L*..&...!.....,...`.....9..i....Q4.....H..j.=.k9-5_.. .....j7..({.....!.....,...`.....9.....trV.....H....`.[.q6.....>.. .CZ.&!.....M...!.....,...`.....8.....:.....H..jJ..U..6_...../.el...q.)...*..!.....,...`.....9.....i..l.go.....H..*".U...f....._.....5 .....n..!.....,...`.....:..i...../.....H...5%.kE/5.....In.a..@&3.....J...!.....,...`.....9.....kr.j.....H..*.-.{Im5c.....@&.....!.....,...`.....9.....j..q....H...].&..\.5.....8..S.....!. .....,...`.....9.....3q.g..5....H...:u.....Al..x.q.....!.....,...`.....9.....\.F....z....H...zX...ov.....h3N.x4.....j..!.....,...`.....9.....Q.:.....H....y..^...1.....n.!.F.....E...!.....,.. ..`.....8.....i,.....H....*_.21.I.....%...

Chrome Cache Entry: 226

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+qLG3W0KviYVsCZu4GvCbJ7I2SVH:jAmlW7t6hOqB08tt7I2SF
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: 227	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	183
Entropy (8bit):	4.91551109797976
Encrypted:	false
SSDEEP:	3:4ovtrKIvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLtjYWRZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EGWeiWoTZHTV
MD5:	6895548091748CFCF47BE6560216595A
SHA1:	A721FE8074CF3BCEB53A810AA9C4C20B7E326A15
SHA-256:	D320CA79C98D26B2847C2EAABBDDB45B932A681603213D3C44DD7491E6CAE443
SHA-512:	6970E70857CAF2A3189A26C36995FE4A61B9EC613C0F37307B2B4AE5DC14F9EB3295281D3CE59146999ADCC9BEEA4F5A3E0645A98CA1D07DD123A255FB63832
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJ4h&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":false,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 228	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	813
Entropy (8bit):	0.3777162536454919
Encrypted:	false
SSDEEP:	3:CUDu//tylaJqAlTlmhy:EX7JqAcy
MD5:	DBC2B30ECD3CE2A7A8965E5B0A569DFF
SHA1:	C32D2FFDBF66B5582C8C184E0C0B436048292807
SHA-256:	9397D5506D9BB44184A4BD44001382209441BD80D8C5FB4F3DFFDB1F966B7995
SHA-512:	496E07788F07A4F31E690E67367086FBAA934CFAEF0256F669B395ADF0EBF8C677D3775BEAB50F5100D178B67F51F5F2AAA7CE8B89EC5B93CAE6F3B2C21BFD6F
Malicious:	false
Reputation:	low
Preview:	GIF89a..... ....!.....,..... .....;

Chrome Cache Entry: 229	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223

Entropy (8bit):	5.214716189224774
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH1l/njMlZLDo8g6n:MMHdVBKW/UTKnj+K6
MD5:	7635A19C1AE1E359DF9BE1412E7F680A
SHA1:	9A1D1D1EEEA2831D6826EE84C55A97689CE68220
SHA-256:	7E5ABAA8FA0DEB978704AC1B37D1B4262DBE7FB98E60E387A807A5C67FA45D82
SHA-512:	74ABBD2E3DFF5D913457C48F221B9E970E737348F0830C9407E985AF7A6BF3E66D986AD28777057F0E1865F6637CD55DB2E33385159DD2847FEE08C2DEC6923A
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/images/webcontrols.png
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:6d3887ed-001e-0001-366f-5b951d000000.Time:2023-03-20T21:03:57.1267159Z</Message></Error>

Chrome Cache Entry: 230

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	downloaded
Size (bytes):	1807
Entropy (8bit):	4.786841370509379
Encrypted:	false
SSDEEP:	24:TEiupF0iupFUhUhUhUdJUhUhUhUhUSUhUhUhU+1iujzqF2:TEioCio41i6r
MD5:	2AE6836529D03D3D791E36C06AE1C098
SHA1:	4AD57A6504DBCDA3F84C89663854DCADFC47FE78
SHA-256:	6B195E4BB92C4713407E0580B500DAA3C6E20AE67FF9984A3F3015DCFA4C6BD7
SHA-512:	945DA3AD60B5F3D8B67AAF2286E490E46FE682732280164EBEF3765D0ED0B72B9FC1D024F4825AFEBD013969E8550000ADC9F4D9BF5D4D53BDB2D82977EA92B
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZD-k&sid=bafhQb8luy6TyutvAC5k
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},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"13924919","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{

Chrome Cache Entry: 231

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):	89590
Entropy (8bit):	5.193479693663803
Encrypted:	false
SSDEEP:	1536:x7cx5Yu0kcI4OtiiB2ZaJUx3qVnS8auwqme2cumAaUmE4Y/rHww1erQ+Hfx07im4:+QROliB2ZAYuwtjR1ec+y7imfg
MD5:	A55B9665B3C5DACA296C27422BF152FA
SHA1:	9220BE1BC39C3ED05FC5CF25D825B8B3A171FCD2
SHA-256:	5B53C6DB5ABDA0AEAD4DEB08A073B3A982E4CEE523A0D5FC2DC69473CD6EFB36
SHA-512:	7950DD0060557B299CEC6D6FD18F89F264E45D8A39E84F97EBB365DC8205ACD4119E7141E0C1867F99BE03D45722D57102D4368DC6E9BA65FCE194B8B24EBF4
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/jsc/controlbundle.js
Preview:	var TextBox=window.TextBox||function(){var r=function(i){var u=t(i),r=n(i),f=i.value;return r&&f.length-u.length>=r?!1:!0},u=function(t){var i=n(t);return i?!1:!0},f=function(r){var u;if(window.clipboardData&&(u=n(r),u)){var f=r.value,e=t(r),o=u-f.length+e.length,s=window.clipboardData.getData("Text").substr(0,o);return i(r,s),!1}return!0},e=function(t){var i=n(t),r=t.value;i&&r.length>i&&(t.value=r.substring(0,i))},n=function(n){var t=n.attributes.multilineMaxLength;return t?parseInt(t.value):null},t=function(n){var t,i;return n.document?(i=n.document.selection.createRange(),t=i.text):t=n.value.substring(n.selectionStart,n.selectionEnd),t},i=function(n,t){var r,i;n.document?(i=n.document.selection.createRange(),i.text=t):n.value=n.value.substring(0,n.selectionStart)+t+n.value.substring(n.selectionEnd)};return{OnKeypressHandler:r,OnBeforePasteHandler:u,OnPasteHandler:f,OnBlurHandler:e,GetMultilineMaxLength:n,GetSelectedText:t,SetSelectedText:i}}();var HelpCallout=window.HelpCallout||fu

Chrome Cache Entry: 232

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (19359), with no line terminators

Category:	downloaded
Size (bytes):	19359
Entropy (8bit):	5.35607110353059
Encrypted:	false
SSDEEP:	192:yOpa6YINNhVOqZ9N2283PLfdKrvdq0W2vm1X+Hlw7qZOsO/qLLLa3tWL2/ydZKxm:yOpbNq8ktRKzJpBueOshvmky/y2r4hwm
MD5:	6CC84268B6A0FDE32739545E28A6B41C
SHA1:	BA8C913DDC576B884C70971EE7876ECF965C28C7
SHA-256:	2EB1A1556AFBD2093E25F9E255CAC9F64E42F4FFB5827BC0459E39D597CFACF0
SHA-512:	C1F2E826E3240DF40EAF623AB0C0D601D0C115CD53B1AFE0960AF7EAE0B212B66C4994F9FDD4724720C718E9FDF9FEE7D30F909896B67CBA9989E241EC67E56D
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/officehub/bundles/staticscripts-6cc84268b6.js
Preview:	var FlushUtilities=function(){function e(){}var n=function(e,n){return n&&n.message?e+": "+n.message:e},t=function(e,n){var t=document.createElement("title");t.innerHTML=n,e.appendChild(t)},i=function(e,n){if(e&&history&&history.replaceState){var t=history.state||{};history.replaceState(t,n,e+window.location.hash)}};return e.redirect=function(e){e&&(window.location=e)},e.onShellInfoLoaded=function(e,r,o){var a=[];try{i(r,e)}catch(e){a.push(n("Caught exception while updating path and query string ",e))}try{var l=document.getElementsByTagName("head")[0];t(l,e)}catch(e){a.push(n("Caught exception while setting page title and appending Shell css to <head>",e))}try{var d=document.getElementsByTagName("body")[0],s=document.createElement("div");s.style="display: none",s.id="ShellInfoLoaded",d.appendChild(s)}catch(e){a.push(n("Caught exception while creating ShellInfoLoaded element",e))}try{window.ng2EventService&&window.ng2EventService.broadcastEvent({name:"shellInfoLoaded",args:[]})}catch(e){

Chrome Cache Entry: 233

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 109863
Category:	downloaded
Size (bytes):	32195
Entropy (8bit):	**7.993880801346853**
Encrypted:	**true**
SSDEEP:	768:uNLJwALnG54pjKKsd9XdKwEXRJexr3yani0:uxTLnG54pdsd9Xd0Tma0
MD5:	039CD406CB780BD9DAE8410D38CE69CB
SHA1:	5DEFD37654F47F6DF5E104D3A34BCB3C1E307A1D
SHA-256:	16C6585A09A7E87B4CB30718E8BDA247C78FFBE590A8043FFE8ECC486270D2D4
SHA-512:	DC2A2B2FE9B02E35537902F65869D35D051F0F720B9BB4D4726D5EDE15B6611D4F12389242350515023C032CA98FD1ED406A694FFD894DFAB7B059F06BFCA84
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pcustomizationloader_aeb718e8cbcfba8bf6ed.js
Preview:	.....z.H.(.....V....H.b.$.]...l...s..,....P..6..."..7"..$).....".."...DFFFD..........._...o.^..z.....z.O.m.|....g.o.;...].Ek.'.../..-ZY...V..|..Q..5...Q.Z..u..b.U....e.J...X.}ny.\.h....._.)|=.V7..I.Y..Y+J..Z..i.ZU.`y..U<.j.....e+gs...N.....V..V...2..+>.^.-.....0.O...\.D._.`...W.L.....g.B5....*..MV.....e..v]P?X...!,.y..Y....1IZ.T.[.....b_VP.HnZ.y.".ew.p.e..5K.....V|.....+.l.b..-5.9.XO.A..{.....E....'..q.?.....\.....z...`.U.IT....ar...|..e.....j.z]]..Z?e.Q..^...nA....+.....{....?.....q..l...V.....V..l.>...UU\y...g.....J.8+..e...."X.0..~.....9.....<|....8.{..<...a.{[.JO+X.....%{.....}...xWe....!..V.?Ee.$....ZK.$ge...F+....+._./oX....q..../>)z9CJ..cQ.....T[iP....KV..'#..3@.|w.b...T?...A..V.....F?.....YV..Cv..Y..]<.}s.kb..M.....(N..9....$.ze'..8....@/..{...K..k..G.T.l..m|...z..R....W`..as~...Xz..v...Y.....S.eoNh.....0.e....E.[h.....+.]so.).vU.....H.....,4.7.|.@h@..|.{.|&...`..Q...X..o..

Chrome Cache Entry: 234

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.911046379915681
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLt4JdZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EoyiWoTZHTV
MD5:	3A1354A50D4950EA728C84B623B2ECDC
SHA1:	ED0A9680DF4BC76019C6271555228C53AD03F766
SHA-256:	234B4EEF13DFB1C06F63FDE4EE694E71E4A76CD7F26E0206DF0633B4268742D4
SHA-512:	A3CA6CAB5316684CC2CE4DA273B09A52D4F80C1069157B7DD675CE43EFB7978860D6AF70771888ED1E1999FA27C856100CC6B1F458DDFBFB17CD15BC1C2A7CB
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZLrA&sid=bafhQb8luy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 235

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:U6OZDyZGokJpZZqOVr4LXQvRn8Il2sK5KcF8NcdKP66Po0Nhdh9e0Zup39sDlrG1:U6OZ5nJpZZqY8gvRn9MKlu8N3P6cVhrE
MD5:	5014BD57D455109B69EC9B55F8F846C2
SHA1:	737038FCE3C91AFDBE4EC5E92F9122B66FFA9003
SHA-256:	A35DE03842CE1919D276CDCBEA23ECC2D247932710B92490E08B5BEDE398E28E
SHA-512:	00BA68BB5CDE01C65C03F75AA459F02322F7B6F4E703E9B35BE46EEB4F9FC1F3F051B6A3088E835A8C5840AEB6814673694CC851A70C1DD9221F455327FDEC0 3
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.._.@).....$....q...M.:....e.1...bd.K...&..P.i.....`!....[....O. Q_l@.....D._.3.6.v.....9$..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: 236

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: 237

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65399)
Category:	downloaded
Size (bytes):	93146
Entropy (8bit):	5.265820615168494
Encrypted:	false
SSDEEP:	1536:ElQF9RJBsvCipiGzxaUCZaq0s6DPINAx9DmLhgfYsTDTkVRWd1M4tgUVA06fu:ECRJDNizWRF4XYfu
MD5:	2C84DDD7EB49D7F61BE23D6FC145887A
SHA1:	38A20CC871F34D86652F7C0C98C9BA6F8DB780A0
SHA-256:	2589FE90B2849F35F294CB20BF433135E44CE0CA8CE98D8E4F0CA7B62FA50191
SHA-512:	8C60683163719094F96A7F363C18D823E83D898C52F7DBA12B34FF5390A0D98057EF31E7392A174F15F435BC1B1C8CF56E0CF322B521C665AAC6BE206E17D13E
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/jquery/jquery-1_10_2_min.js
Preview:	/*! jQuery v1.10.2 with a fix integrated from v1.12.2, 3.4.0, and 3.5.0 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license */.(function(n,t){function ci(n){var t=n.lengt h,r=i.type(n);return i.isWindow(n)?!1:1===n.nodeType&&t?!0:\"array\"===r||\"function\"!==r&&(0===t||\"number\"==typeof t&&t>0&&t-1 in n)}function ue(n){var t=pi[n]={};return i.each(n.match(s)||[],function(n,i){t[i]=!0}),t}function ou(n,r,u,f){if(i.acceptData(n)){var h,o,c=i.expando,l=n.nodeType,s=l?i.cache:n,e=l?n[c]:n[c]&&c;if(e&&s[e]&&(f||s[e].data)||u!==t||\"string\"!=typeof r)return e||(e=l?n[c]=b.pop()||i.guid++:c),s[e]||(s[e]=l?{}:{toJSON:i.noop}),(\"object\"==typeof r||\"function\"==typeof r)&&(f?s[e]=i.extend(s[e],r):s [e].data=i.extend(s[e].data,r)),o=s[e],f||(o.data||(o.data={}),o=o.data),u!==t&&(o[i.camelCase(r)]=u),\"string\"==typeof r?(h=o[r],null==h&&(h=o[i.camelCase(r)])):h=o,h}}fu nction su(n,t,r){if(i.acceptData(n)){var e,o,s=n.nodeType,u=s?i.cache:n,f=s?n[i.expando]:i.expando;if(u[f]){if(t&&(e=r?u[f]:u[f].d

Chrome Cache Entry: 238

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text

Category:	downloaded
Size (bytes):	215
Entropy (8bit):	5.296544088357521
Encrypted:	false
SSDEEP:	6:JiMVBdgqZjZWtMfgRTH152ywqlDGAAg6n:MMHdVBZWyUTqIGAF6
MD5:	777ED0F978A3A214D54CD5A22067BDE9
SHA1:	D03207856BAE932516B8034214BC359E263E25AA
SHA-256:	9DDD56174ECF88DF6F6332EDF2F70BBA4EDC2181D9D8216C9F0C6564091EF822
SHA-512:	E36A4B1ED451941B6C949652975C22354BEDD45D609B37C539912F590EB9CA89C68E7562116051DE2E745F9683C6B0DF58EA64460A65BF1C9B64D2642C03EC8
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/webtrends.js
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>BlobNotFound</Code><Message>The specified blob does not exist..RequestId:6c6a4546-e01e-006b-176f-5b4d35000000.Time:2023-03-20T21:03:40.4236241Z</Message></Error>

Chrome Cache Entry: 239

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

Chrome Cache Entry: 240

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (31932)
Category:	downloaded
Size (bytes):	53160
Entropy (8bit):	5.382742628871051
Encrypted:	false
SSDEEP:	768:Jmn+Bh5LkzObU/cOTEShONa7zUdvHCIsbzwzOu1jxYrJr0lBt7N41ZkBgu8vUDaE:TBh7bU0OTEShONytI5zjDlEQT
MD5:	FF1C847AF56181C2382E6EF53D374A55
SHA1:	0BC31FC15822B090BB7F5FCBEB1A9B44EE14D3DD
SHA-256:	87CB590BC4F521F9B76C44104DC7AB28B34EB25E3AB82A49137661EEC47A27BD
SHA-512:	6F7FC7D0133E11A911635C2C9BA8FEEEC54CA52F145A342D6B2F2CDA533A7BCC3D8DB9E792A6C9DA6E761828C4F53686AF48CE381D1A4BD490F6A24DBBB91B24
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/officehub/bundles/sharedscripts-ff1c847af5.js
Preview:	!function(e,t){if("object"==typeof exports&&"object"==typeof module)module.exports=t();else if("function"==typeof define&&define.amd)define([],t);else{var i=t();for(var n in i)("object"==typeof exports?exports:e)[n]=i[n]}}(this,function(){return function(e){function t(n){if(i[n])return i[n].exports;var r=i[n]={i:n,l:!1,exports:{}};return e[n].call(r.exports,r,r.exports,t),r.l=!0,r.exports}var i={};return t.m=e,t.c=i,t.i=function(e){return e},t.d=function(e,i,n){t.o(e,i)||Object.defineProperty(e,i,{configurable:!1,enumerable:!0,get:n})},t.n=function(e){var i=e&&e.e?function(){return e.default}:function(){return e};return t.d(i,"a",i),i},t.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},t.p="",t(t.s=30)}([function(e,t,i){"use strict";Object.defineProperty(t,"__esModule",{value:!0}),function(e){e[e.Unspecified=0]="Unspecified",e[e.String=1]="String",e[e.Int64=2]="Int64",e[e.Double=3]="Double",e[e.Boolean=4]="Boolean"}(t.AWTPropertyType||(t.AWTPropertyType={})),function(e

Chrome Cache Entry: 241

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

Category:	downloaded
Size (bytes):	183
Entropy (8bit):	4.91551109797976
Encrypted:	false
SSDEEP:	3:4ovtrKIvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLtjYWRZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EGWeiWoTZHTV
MD5:	6895548091748CFCF47BE6560216595A
SHA1:	A721FE8074CF3BCEB53A810AA9C4C20B7E326A15
SHA-256:	D320CA79C98D26B2847C2EAABBDDB45B932A681603213D3C44DD7491E6CAE443
SHA-512:	6970E70857CAF2A3189A26C36995FE4A61B9EC613C0F37307B2B4AE5DC14F9EB3295281D3CE59146999ADCC9BEEA4F5A3E0645A98CA1D07DD123A255FB6383 2
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZZVI&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":false,"userId":"2","name": null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 242

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (65339), with CRLF line terminators
Category:	downloaded
Size (bytes):	659798
Entropy (8bit):	5.352921769071548
Encrypted:	false
SSDEEP:	12288:nEMsQrWEWbnByixmwgXZewhYcFiG4DUIxo:nEMsJpBJgHKcFQNo
MD5:	9786D38346567E5E93C7D03B06E3EA2D
SHA1:	23EF8C59C5C9AA5290865933B29C9C56AB62E3B0
SHA-256:	263307E3FE285C85CB77CF5BA69092531CE07B7641BF316EF496DCB5733AF76C
SHA-512:	4962CDF483281AB39D339A7DA105A88ADDB9C210C9E36EA5E36611D7135D19FEC8B3C9DBA3E97ABB36D580F194F1860813071FD6CBEDE85D3E88952D099D68 05
Malicious:	false
Reputation:	low
URL:	http://https://r4.res.office365.com/owa/prem/15.20.6178.37/scripts/boot.worldwide.1.mouse.js
Preview:	.window.scriptsLoaded = window.scriptsLoaded || {}; window.scriptProcessStart = window.scriptProcessStart || {}; window.scriptProcessStart['boot.worldwide.1.mouse.js'] = (new Date()).getTime();..;_a.d.G=function(n,t){this.b=n;this.a=t};_a.d.G.prototype={b:0,a:0};_a.fo=function(n){this.s=n};_a.fo.prototype={s:null,t:null,i:function(){return this.s.currentTarget},e:function(){return this.t?this.t.x:this.s.pageX},f:function(){return this.t?this.t.y:this.s.pageY},o:function(){return this.s.relatedTarget},b:function(){return this.s.target},n:function(){return this.s.timeStamp||+new Date},a:function(){var n=this.s.which;!n&&_a.o.a().K&&this.s.type==="keypress"&&(n=this.u());return n},u:function() {return this.s.keyCode},m:function(){return this.s.originalEvent},j:function(){return this.s.type},k:function(){return this.s.originalEvent.touches},q:function(){return this.s.isDef aultPrevented()},g:function(){return this.s.shiftKey},h:function(){return _j.G.a().P?this.s.metaKey:this.s.ctrlKey},l:

Chrome Cache Entry: 243

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	5.270348975644711
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8DHgWdzRiAU2uvxV1tlS4pJQDd0lZLG9ZQg6n:MMHdVBMHgWdzR05tSpJWdmQ16
MD5:	16646042D223750E6ADC26E33D8C122A
SHA1:	8231906269C787D00B74DE181AF896601ADC0DA5
SHA-256:	0C3B42E8653D5EE7F84B3FDA2E2B95B004B45C717A41CC94C4A26B65EE0A39B8
SHA-512:	51BF6D08A4BB146602A839CB4817409E914CABA9F0E413B35C11C2EC7BA82DC9D8394A7200FD740E7927E50E12D264C9A7333B79CC85C7DCCEE27CAA4E62A A3
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/Shell/Images/header_wizard_hl_mos.jpg
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>OutOfRangeInput</Code><Message>One of the request inputs is out of range..RequestId:52edbd86-301e-0028- 346f-5b9e3f000000.Time:2023-03-20T21:03:57.1450238Z</Message></Error>

Chrome Cache Entry: 244

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

Size (bytes):	182
Entropy (8bit):	4.911046379915681
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLt4JdZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EoyiWoTZHTV
MD5:	3A1354A50D4950EA728C84B623B2ECDC
SHA1:	ED0A9680DF4BC76019C6271555228C53AD03F766
SHA-256:	234B4EEF13DFB1C06F63FDE4EE694E71E4A76CD7F26E0206DF0633B4268742D4
SHA-512:	A3CA6CAB5316684CC2CE4DA273B09A52D4F80C1069157B7DD675CE43EFB7978860D6AF70771888ED1E1999FA27C856100CC6B1F458DDFBFB17CD15BC1C2A7CB
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZK3M&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 245

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2952)
Category:	downloaded
Size (bytes):	107301
Entropy (8bit):	5.394768749747235
Encrypted:	false
SSDEEP:	3072:T/nVnkYX6SnT0V2XohxoC2XSj2XvwzPXZoPXaUu0hAytG/gi:xX6sTKfUuaNi
MD5:	2AD03DB2F559D6E2A57AD1CFF94E2FE4
SHA1:	A6C5D1BF10C3DC1FED2330FEBDA225B79A09124C
SHA-256:	528CD29517DAA37E4C7DA91E446A7401A981DE1ACC2A1FC54640AB2279206832
SHA-512:	115B1C6BD341BD70A56C537956DC595121FDA74B226C8FC94AFF445F75DD3439D776314598DCC088D59A05975E191AAAC567B3877F23518C7A6630862488A0D
Malicious:	false
Reputation:	low
URL:	http://https://acctcdn.msauth.net/resetpasswordpackage_KtA9svVZ1uKletHP-U4v5A2.js?v=1
Preview:	function Encrypt(e,n,t,o){var r=[];switch(t.toLowerCase()){case"chgsqsa":if(null==e||null==n){return null}r=PackageSAData(e,n);break;case"chgpwd":if(null==e||null==o){return null}r=PackageNewAndOldPwd(e,o);break;case"pwd":if(null==e){return null}r=PackagePwdOnly(e);break;case"pin":if(null==e){return null}r=PackagePinOnly(e);break;case"proof":if(null==e&&null==n){return null}r=PackageLoginIntData(null!=e?e:n);break;case"saproof":if(null==n){return null}r=PackageSADataForProof(n);break;case"newpwd":if(null==o){return null.}r=PackageNewPwdOnly(o)}if(null==r||"undefined"==typeof r){return r}if("undefined"!=typeof Key&&void 0!==parseRSAKeyFromString){var a=parseRSAKeyFromString(Key)}var i=RSAEncrypt(r,a,randomNum);return i}function PackageSAData(e,n){var t=[],o=0;t[o++]=1,t[o++]=1,t[o++]=0;var r,a=n.length;for(t[o++]=2*a,r=0;a>r;r++){t[o++]=255&n.charCodeAt(r),t[o++]=(65280&n.charCodeAt(r))>>8}var i=e.length;for(t[o++]=i,r=0;i>r;r++){t[o++]=127&e.charCodeAt(r)}return t}function PackagePwdOn

Chrome Cache Entry: 246

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 1378
Category:	downloaded
Size (bytes):	628
Entropy (8bit):	7.6610853322771
Encrypted:	false
SSDEEP:	12:X6/EjXb5e1vpPDySPLiDB/3YLZzrlDuLRndk6l3WZi1epo7IyhadSH8Ib1yfuI:X6cP5e3dgYLMk69li1epryt/Md
MD5:	6F68E9881DF18F8E251AB57D5786239B
SHA1:	C0F7A01A288752833390FC330995F25488BCE8EC
SHA-256:	B33E30351B2F4EF67D53D2C6DBE189A4D572425037E4F1264A0190DC4A820845
SHA-512:	B33DFF67480DF940FA0565B231E02F26840DCB5135A4A2FF3C310AA062D3D4B456FA9C8C6E2BC59EC76B515EA1B36D574A5701771BCEE7CEE97B99EF60A803C6
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_account_aad_f83ebff69a4a1685e4dc9650cdab8886.svg
Preview:	.....m.Mo.0.....]%F..6...rX.;..&i..].&HZ...#%...B..4.W$.....>....v8...f....g.O/.3k....ms.o....m...a8.....u..4>.]....r~8...%.....x.m.y].....u.>..7....l.]....i..fC.[O..z.)..r.....g!(.+....4.P9.0@.....R.....^q.l[..7.....Q;...6.N....a.d.%....:...6FE.}.....}s.`LV..Q.U. 8..}..y.&..l..a.\.8%..kgoo.Q6...>.5.8..!.....".t9].v.B) `.G6.V.E\..AJQU.7...J.oS.*.....*.*@.....l.....{.r..KP@.....9YD..U.....&..:..d.....+/...(..:.S_...S.....n..z.a...,.,&VB.....eJR)...R.H3])>....9O.....KDi.O..#...-?D.1*..N.p....h.#.Z.[/..!.h..$..S..Phdqd....}.....E>g..q5..J.T.....u.....i.b...

Chrome Cache Entry: 247

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2773), with no line terminators

Category:	downloaded
Size (bytes):	2773
Entropy (8bit):	5.002767825703638
Encrypted:	false
SSDEEP:	48:TEishfRzibCLRCoRCKNTiaACFlOcCgQgOcCaLpsXEo1ACSc+kd4sJLkwwTd:1KfRzPLYoYKNTNyOZDgOZaLps0MNSYiP
MD5:	39D8506B201CCD35E51DB3C572950E24
SHA1:	850B96A4EB34062FCE298CB0B995476E721E3BF9
SHA-256:	ACD515F6E3C7C754333CD1F4B22912D5B490C408F8FF485FC2724F622E255977
SHA-512:	AE6E1B6467AACDE647FFFB1877FA3278C6B5683FF7F91218AB51CA6A7045C6345B361F6CB952784B6F9D6DB856948A5D7A4630B6578B2AF49A4F7081D68D877
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZC8Y&sid=z5Pk-iNyt0hd5jCcAC5e
Preview:	42["message",{"component":"PM_DOC","type":"CLIENT_VARS","response":{"error":null,"data":{"boxCommentsCount":0,"collections":[],"doc":{"type":"doc","attrs":{"table_of_contents":{"enabled":false,"allowedLevels":[1,2,3]}},"content":[{"type":"paragraph","content":[{"type":"text","marks":[{"type":"font_size","attrs":{"size":"1.75em"}},{"type":"strong"},{"type":"author_id","attrs":{"authorId":"24404463343"}}],"text":"Check below for the vital document shared"}]},{"type":"paragraph"},{"type":"paragraph","content":[{"type":"text","marks":[{"type":"font_size","attrs":{"size":"1.5em"}},{"type":"strong"},{"type":"author_id","attrs":{"authorId":"24404463343"}}],"text":"PROJECT: TY0923"}]},{"type":"paragraph","content":[{"type":"text","marks":[{"type":"font_size","attrs":{"size":"1.5em"}},{"type":"strong"},{"type":"author_id","attrs":{"authorId":"24404463343"}}],"text":"SUBMISSION: P96390"}]},{"type":"paragraph"},{"type":"paragraph","content":[{"type":"text","marks":[{"type":"link","attrs":{"href":

Chrome Cache Entry: 248

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (38677), with no line terminators
Category:	downloaded
Size (bytes):	38677
Entropy (8bit):	5.2403199684773
Encrypted:	false
SSDEEP:	768:mlxte81WzOZm5eiSPuAAjmFl9+pW4bg1WMG1yKyAIHo7lYSF5bsbMb8jssi1+:ix91WzZYiOuIl9+pW4b7lXSo
MD5:	F0CCEF116CC550152B90DB0EA68D8FB0
SHA1:	1D813F3F06C36AA45AE76A8B5AAD50B24FCC460D
SHA-256:	811E2184ACAC6E3DC10851B5E1DDD6F431AB4FEFF39A4914EE487A961F7761DB
SHA-512:	2105C19E40EE71D0278832B430A9E208606AFE052F6C05A3CE53D5B2F31E114246853E836A971891F1EA9B7165EC08D63F9F4B516D141BC8E7DBC0073240F72A
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/jsc/hipcontrol.js
Preview:	function HipChallenge(){this.LoadingTrials=3,this.CurrentLoadingAttempt=0,this.FailOverMessage='',this.ShouldShowMessageOnFailing=!0,this.IsActive=!1,this.IsUILess=!1,this.IsChallengeLoading=!1,this.ChachedLoadingParams=!1,this.CachedLoadParam1=null,this.CachedLoadParam2=null,this.CachedLoadParam3=null,this.ChallengeId='',this.Verified=!1,this.FailOverChallengeId="",this.LoadTimeOut=2e3,this.LoadTimeOutHandle=null,this.UILoaded=!1,this.PrerequisiteChallenge='',this.ConnectionFailed=!1,this.ShowValidation=!1,this.Loaded=!1,this.DependantChallengeId='',this.GradedActionChallenge='',this.ShowErrorPanel=function(){},this.Deactivate=function(){},this.Activate=function(){},this.ShowConnectivityError=function(){},this.GetVerificationData=function(){this.NotImplementedException()},this.GetUserResponse=function(){this.NotImplementedException()},this.GetChallengeType=function(){},this.Show=function(){this.UILoaded=!0},this.Hide=function(){this.UILoaded=!1},this.Verify=function(){return!0},this.V

Chrome Cache Entry: 249

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/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZRFx&sid=bafhQb8Iuy6TyutvAC5k
Preview:	2

Chrome Cache Entry: 250

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: 251

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.911046379915681
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLt4JdZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EoyiWoTZHTV
MD5:	3A1354A50D4950EA728C84B623B2ECDC
SHA1:	ED0A9680DF4BC76019C6271555228C53AD03F766
SHA-256:	234B4EEF13DFB1C06F63FDE4EE694E71E4A76CD7F26E0206DF0633B4268742D4
SHA-512:	A3CA6CAB5316684CC2CE4DA273B09A52D4F80C1069157B7DD675CE43EFB7978860D6AF70771888ED1E1999FA27C856100CC6B1F458DDFBFB17CD15BC1C2A7CB
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZIhy&sid=bafhQb8luy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 252

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (45991), with NEL line terminators
Category:	downloaded
Size (bytes):	100459
Entropy (8bit):	5.372466567338347
Encrypted:	false
SSDEEP:	768:lsJ3687fBEc408QYHLMzPnLtedvj39MtqOh2eMrFGob/fmltYUyGSGk8n:lkK4mm/8LMDyj39MPCrF3b/elBycn
MD5:	C9779318B90DEBA5DA366F290FFC3CCC
SHA1:	8EC148193F694FD726F99388AE4211667CD2F011
SHA-256:	1091C540F20FE092D78890E207CD6F9C6994041BA4C3167AE6E8FF658DE55BBC
SHA-512:	80D4BC30FB69941AC3DFAA2E13F0997FBBCADEF57A06B8D134DBD274935313CA170EBF2DCAD1F87335AA3D4A27E9703B5CA7EA3F79E32D5014093ED120232C9
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/officehub/bundles/polyfills-bundle-fa84912a3000089af4a8.js
Preview:	!function(t){var r={};function n(e){if(r[e])return r[e].exports;var o=r[e]={i:e,l:!1,exports:{}};return t[e].call(o.exports,o,o.exports,n),o.l=!0,o.exports}n.m=t,n.c=r,n.d=function(t,r,e){n.o(t,r)||Object.defineProperty(t,r,{enumerable:!0,get:e})},n.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},n.t=function(t,r){if(1&r&&(t=n(t)),8&r)return t;if(4&r&&"object"==typeof t&&t&&t.__esModule)return t;var e=Object.create(null);if(n.r(e),Object.defineProperty(e,"default",{enumerable:!0,value:t}),2&r&&"string"!=typeof t)for(var o in t)n.d(e,o,function(r){return t[r]}.bind(null,o));return e},n.n=function(t){var r=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(r,"a",r),r},n.o=function(t,r){return Object.prototype.hasOwnProperty.call(t,r)},n.p="",n(n.s=1)}({"+5TE":function(t,r,n){"use strict";n("Muwe");var e=n("0K2p"),o=n("+iL7"),i=n("GHf2"),a=

Chrome Cache Entry: 253	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	194
Entropy (8bit):	5.014114983792889
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gfqKPv3ULWAlHxAQWAXc13TwJQ3UFExGBdxPls2stEtAp6Vn:4ovMwl/m2mX3EADyG3GX1dU
MD5:	F370E30DC1DAB486C60B724AF0F410A9
SHA1:	D4370031DA06A97C28B6ED586F86CF501E856A3A
SHA-256:	D87F086251B8BC81B39E311BBAEC832AA5E56FF24738A59BF0EBA2EE3EAA1231
SHA-512:	2026BA907A22EF38889F6C5451C8E792A58E0465A7387F0080489712764A651AE00143A2E502F2351306DDF6B28767507594CA37E12634FFA050E1852B9312BD
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJjl&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USER_CURSOR_CHANGED","response":{"error":null,"data":{"userId":"24404463343","userPosition":{"head":198},"docVersion":10,"docOrSelHasChanged":false}}}]

Chrome Cache Entry: 254	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.911046379915681
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLt4JdZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EoyiWoTZHTV
MD5:	3A1354A50D4950EA728C84B623B2ECDC
SHA1:	ED0A9680DF4BC76019C6271555228C53AD03F766
SHA-256:	234B4EEF13DFB1C06F63FDE4EE694E71E4A76CD7F26E0206DF0633B4268742D4
SHA-512:	A3CA6CAB5316684CC2CE4DA273B09A52D4F80C1069157B7DD675CE43EFB7978860D6AF70771888ED1E1999FA27C856100CC6B1F458DDFBFB17CD15BC1C2A7CB
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZYUF&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 255	
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/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZG8i&sid=bafhQb8Iuy6TyutvAC5k
Preview:	2

Chrome Cache Entry: 256	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (7600), with no line terminators
Category:	downloaded

Size (bytes):	7600
Entropy (8bit):	4.755347264022592
Encrypted:	false
SSDEEP:	96:gTJ0Z6QYvW81oyLEfqSorX5Kjb6tk63LA5D287sq5pY+0dnk3P54aaoJ99orOoY0:S0dYjueAynT8js
MD5:	BC6A941A872D57146E13823F6935A7F2
SHA1:	E648D16D68417B81616454539EDD8303E04DBEC7
SHA-256:	D132D49C1C8945F5C43AE470BADF2B6EDCD584297E84E59DD2034FFB7DC863B3
SHA-512:	F9629A3E82E24FC48DEA4C677491235AAB0098CEDF40DB9F98E53CA430B5DD105A2D9F092E007351AFE2BCCCD2A430C9020EDAE55665E3F3517703A3D00CDE 71
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/css/o365themedefault.css
Preview:	.o365-theme-base,.o365-theme-base input,.o365-theme-base textarea,.o365-theme-base select{background-color:#fff;color:#333;border-color:#666}.o365-theme-base h1 ,.o365-theme-base h3,.o365-theme-base h4,.o365-theme-base h5,.o365-theme-base h6{color:#333}.o365-theme-base h2{color:#666}.o365-theme-base a{color:#0 078d7}.o365-theme-base input:focus,.o365-theme-base input:hover,.o365-theme-base textarea:focus,.o365-theme-base textarea:hover,.o365-theme-base select:hover,.o 365-theme-base select:focus{border-color:#2b88d8}.o365-theme-base a[disabled],.o365-theme-base a[disabled]:hover{color:#666!important}.o365-theme-base input[dis abled],.o365-theme-base textarea[disabled]{background-color:#f4f4f4;border-color:#eaeaea;color:#a6a6a6}.o365-theme-base input:disabled,.o365-theme-base textarea :disabled{background-color:#f4f4f4;border-color:#eaeaea;color:#a6a6a6}.o365-theme-base input[type=submit]{background-color:#0078d7;border-color:#0078d7}.o365-th eme-base .DataTable td,.o365-theme-base .DataTable

Chrome Cache Entry: 257

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 379
Category:	downloaded
Size (bytes):	254
Entropy (8bit):	7.066074991728423
Encrypted:	false
SSDEEP:	6:XtS8G99k8e6my4IIFqXUJ59IDFCnhUGIZX8My/dOtrE:XAH99kRX1YQBDFCnDXdWYtrE
MD5:	847A4212B99B9076EE39328B24CD30AF
SHA1:	73F15078CF1D396485F644A79B6E25EF0637685D
SHA-256:	29DC0C26C372805325EB7EB926769E832A60B47BEF96A66436EC3EC05CD6128E
SHA-512:	9AF77E9ED8BD9A39A47F36AAC2D01B5AF5D56C04CD933427DF95CC80904D7EE7AC3F7F9443D8AEF236CC84FB4DC4CC335AF0BF8F9BC0C13D720187096D149 20
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_account_msa_2d8f86059be176833897099ee6ddedeb.svg
Preview:	.....mP.n. ...D.xY0.\..{. 7...y.F!.....T..Y.Y..n...q^.[O}..w.SJ.j..3.....%)....x.f.K}..}\.=E.D....!.n.....Ma..G.=+.%.w..WX...9.A.....X...V...bOB&2.H....15{.fT...V-.#..m..f...V2< ...~....l%4.....Ie.TL69.....vW.....v.3.v.O..}..{...

Chrome Cache Entry: 258

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; }..ProseMi rror-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: 259

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

File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD(1
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.....h(..f...HH.....(..00.....h....6.. .....=.....@.....(....A..(.....(.....("P.....""""""""""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""" """"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...33333333333 33333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""" """"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""" ...33333333333 33333333333333333""""""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""""""""

Chrome Cache Entry: 260

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
URL:	http://https://account.live.com/Resources/images/microsoft_logo_7IyNn7YkjJOP0NwZNw6QvQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0- 1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 261

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 3651
Category:	downloaded
Size (bytes):	1435
Entropy (8bit):	7.8613342322590265
Encrypted:	false
SSDEEP:	24:XjtSZi0kq+yVCGYXVrO4vDxik/N/z5VaLPbholJvf6dblke68eRZJyBDz3BnZcNX:XgDkpyVCGca4b//9z5oPXdbl9688qRzY
MD5:	9F368BC4580FED907775F31C6B26D6CF
SHA1:	E393A40B3E337F43057EEE3DE189F197AB056451
SHA-256:	7ECBBA946C099539C3D9C03F4B6804958900E5B90D48336EEA7E5A2ED050FA36
SHA-512:	0023B04D1EEC26719363AED57C95C1A91244C5AFF0BB53091938798FB16E230680E1F972D166B633C1D2B314B34FE0B9D7C18442410DB7DD6024E279AAFD61B
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	.....WMo.7..+..uV.HJ...{.....&...v...(Q.F.....aW.Q.|..~.|{~...b{8...zv.....8|...b.gxb.y{.x<\lS...p...p..l7...o.}.v.....t.....r..r.|9?.....HP...r.4.aGA.j....7.!....K.n.B.Z.C.]....kj..A. .p...xl...b..I!K..><.B..O....#...$.]h.bU.;.Y...).r.u....g*.-w.2..vPh....q....4_..N\..@y).t{.2pj.f..4h.....NC.....x.R..P..9.....".4.`%N..&...a.@.....fS)A4.F..8e9KHE....8d.CR.K..g..Q.....a ....f.....dg*N.N.k..#w.....,.".%..I.q.Y.R]..7.!.:.Ux...T.qI..{..,b..2..B...Bh...[o..[4....dZ.z.!.l....E.9$..Y.'...M.,p..$..8Ns3.B.....{.....H..Se3....%.Ly...VP{.Bh.D.+....p..(..`....t....U.e....2 .....j...%..0.f<...q...B.k..N....03...8....l.....bS...vh..8..Q..LWXW..C.....3..Pr.V.I...^=VX\,d9f.Y;1!w.d,.qvs....f*;.....Zhrr,,.U....6.Y....+Zd.*R...but...."....4.L...z.....L.Q.....).....,].Y .&....*ZsIVG.^...#...e..r....Z..F..c..... .QDCmV..1.~...J9..b_Oov\..X.R..._.TqH.q.5G.0{ZphQ..k...s..\.../.Dp..d`#.....8.#Y...Mb.j.Q.....=n4.c....p.[.SI.....0.N.

Chrome Cache Entry: 262	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 412391
Category:	downloaded
Size (bytes):	114301
Entropy (8bit):	**7.99779365786384**
Encrypted:	**true**
SSDEEP:	3072:KJAEpfLsFCl42xOOax7wkkUcheEByGl9UJPaOEwlw:KiqgFD2xyjCgEBNCxtlw
MD5:	BB47875EB7ACF3BCA0526431119B35B2
SHA1:	8412901F917EAA99887A439E2AFE3B0FAD4F4BC8
SHA-256:	0C452C04F71F1AC96C5BACEB10E9E6A60FBFD5B97E18C5CCFB40D7F6661A9BC7
SHA-512:	1D97554D694B261CB2F01AFADB81556373B9BF0510E3450DF6BE513B250D8F52BA4220F079821DBAB3F78B06D51A824C351554A7FA449A4E429CD299690E9D84
Malicious:	false
Reputation:	low
URL:	**http**://https://aadcdn.msauth.net/shared/1.0/content/js/ConvergedLogin_PCore_EH-q9hPYkBqq2xSfT_DcJw2.js
Preview:	.....{W.H.8....F3.....,Z...U..Lc..Y...R...W.y.....L)%.T...{.....WdddDdd.o._..Wv.....u]..V.....+.....z88..z.Q..../.L=.U...3....0.x..F.0...W..o..~e..O..U.Q.'s...{q..&.._*U..r+.v..U. .z..gP.7..(..7...T.0..V...j..#.Ye.,,..<x.C..s.0..I%b...x...&....J..4....Ze.....-.....\.pJ...0@/....0h,...[M.DZ..7.J.V...}6./.U.oO1...Yu..w.$..0c.=c.}...xT!d....{..@.Uf.. .es0q.,b.....cTt.V .....Qaq....._....$.T*..a...W..z..[....:.zH.yl~.4...O..p1.....<...O.9.].....g.Wf.r1..T..'..d[.*..9._J.....ik....X..K...T.....7<#.....?.;#..c....?.5..... ...=+.....WM.f?...9.=...%.....S.....o o.....S./.*~@+..?...v ..D.wU...TYe.....jp..].#{.;....&U.....e.i.W.).BD.7.z.....d....].:....Pi....g..on5..i.W..Q.a!.c".....u..z..:..P.=.....X.(.....N1.F....@...<D....R...(..i.....I.F< .. T...`1.W3...L..Q.....f.\.....Z.a..%R?.>e..3....=..o..H..*....w/...G.*.....t.0%+.$.Ta.3u#R..y...t....G....z.O?g,9..Go....~bU..4..2.(..%'<B....

Chrome Cache Entry: 263	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	690538
Entropy (8bit):	5.2949544511645605
Encrypted:	false
SSDEEP:	12288:7KWN2vd+Jue9v8E8m8t8E8E8M8m8U08Ehv481usi:7KWN2voJue9v8E8m8t8E8E8M8m8U08E8
MD5:	FE928E5FC1896C48ECB2064F0D5F46E7
SHA1:	67162013B979103FA64740D06D234CBD2852B842
SHA-256:	C1A605BA985EE8298C1421F011454557F1E21AC55559F0490BCF8F3CD7D41CB1
SHA-512:	6510C1F6D887F36D59421E43061DF59C1127731BD9B5B023609A668C16F297940495791B9FEC0D13527EAA4B89AB88A010E8B427394C20346A63D57944CD65C6
Malicious:	false
Reputation:	low
URL:	**http**://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/jsc/adminapp.js
Preview:	Array.prototype.find||Object.defineProperty(Array.prototype,'find',{value:function(n){var i,u,f,t,r;if(this==null)throw new TypeError('"this" is null or not defined');if(i=Object(this),u=i.length>>>0,typeof n!='function')throw new TypeError('predicate must be a function');for(f=arguments[1],t=0;t<u;){if(r=i[t],n.call(f,r,t,i))return r;t++}return undefined},configurable:!0,writable:!0}),Object.entries||(Object.entries=function(n){for(var i=Object.keys(n),t=i.length,r=new Array(t);t--;)r[t]=[i[t],n[i[t]]];return r}),typeof Object.assign !='function'&&Object.defineProperty(Object,"assign",{value:function(n){'use strict';;var f,r,i,u;if(n==null)throw new TypeError('Cannot convert undefined or null to object');for(f=Object(n),r=1;r<arguments.length;r++)if(i=arguments[r],i!=null)for(u in i)Object.prototype.hasOwnProperty.call(i,u)&&(f[u]=i[u]);return f},writable:!0,configurable:!0}),String.prototype.startsWith||(String.prototype.startsWith=function(n,t){return this.substr(!t||t<0?0:+t,n.lengt

Chrome Cache Entry: 264	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (727)
Category:	downloaded
Size (bytes):	2798
Entropy (8bit):	5.027650375532362
Encrypted:	false
SSDEEP:	48:LgEKy5BUYJjqkqIspEagdJBkk/7kVTBp184yMp4kxARbIBzQIuNMeejzA2zjMic4:Lghy1j1ikBJ7EBK+pT90e
MD5:	217EB1AD60A819C4443AC6DBB10D58BE
SHA1:	C95EC188A160D68F8FD17C85CA61536310179D2E
SHA-256:	ECFFBD0C518984B8E77EE5465E882CDDD6B88D7D6A9C5874CF51CBA743229A58
SHA-512:	53192746757F737CFC8008AE94A9BF07758F99090D77B41D27CB2D4ECB137CB694DD8FB168E0E124990FA40B6883C7CC687A81B49FCC790897449CA8BC0332E
Malicious:	false
Reputation:	low
URL:	**http**://https://acctcdn.msauth.net/bootstrapshim_IX6xrWCoGcREOsbbsQ1Yvg2.js?v=1

Preview:	!function(){var e=function(e){var t;return"function"==typeof Event?t=new Event(e):(t=document.createEvent("Event"),t.initEvent(e,!0,!0)),t},t=function(e,t){this.options=t ,this.$element=$PageHelper.get(e),this.$backdrop=this.isShown=null,this.options.remote&&this.$element.find(".modal-content").load(this.options.remote,$PageHelpe r.proxy(function(){this.$element.trigger("loaded.bs.modal")},this))};t.DEFAULTS={"backdrop":!0,"keyboard":!0,"show":!0},t.prototype.toggle=function(e){return this[this.is Shown?"hide":"show"](e).},t.prototype.show=function(){var t=this,o=e("show.bs.modal");this.$element.trigger(o),this.isShown||(this.isShown=!0,this.escape(),this .$element.on("click.dismiss.bs.modal",'[data-dismiss="modal"]',$PageHelper.proxy(this.hide,this)),this.backdrop(function(){t.$element.parent().length||t.$elemen t.appendTo(document.body),t.$element.show().css("display","block"),t.$element.addClass("in").attr("aria-hidden",!1),t.enforceFocus()}))},t.prototype.hide=function(t){t&&t .preventDe

Chrome Cache Entry: 265

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 1864
Category:	dropped
Size (bytes):	673
Entropy (8bit):	7.6596900876595075
Encrypted:	false
SSDEEP:	12:Xl0t8TUViiYi5m6FhSBXWPsigK99WCqKMvBBFThSqfLd81CK6bC+k7LqZLsFlD:XFUVpkNK0Rwid81p6btk7LqZ6D
MD5:	0E176276362B94279A4492511BFCBD98
SHA1:	389FE6B51F62254BB98939896B8C89EBEFFE2A02
SHA-256:	9A2C174AE45CAC057822844211156A5ED293E65C5F69E1D211A7206472C5C80C
SHA-512:	8D61C9E464C8F3C77BF1729E32F92BBB1B426A19907E418862EFE117DBD1F0A26FCC3A6FE1D1B22B836853D43C964F6B6D25E414649767FBEA7FE10D2048D7A 1
Malicious:	false
Reputation:	low
Preview:	..........U.n.0....}i..P..C..7l/..d.....n...G....yl. .E.....Tu.F.....?$.i.s..s...C..wi$.....r....CT.U.FuS..r.e.~...G.q...*..~M..mu}.0.=..&.~.e.WLX.....X..%p..i.....7+.....?.....WN..%>. ..$..c..}N....Y4?..x.1.....*.#v...Gal9.!.9.A.u..b..>..".#A2"+...<qc.v....)3...x.p&..K.&..T.r.'....J.T....Q..=..H).X...<.r...KkX.....)5i4.+.h.....5.<..5.^O.eC%V^....Nx.E..;..52..h....C"l./ .`..O...f..r..n.h.r]}.G^..D.7..i.].}.G.].....{....oW.....h.4...}~=6u..k...=.X..+z}.4.].....YS5..J.....).....m....w.....~}.C.b_..[.u..9_7.u.u.....y.ss....:_yQ<{..K.V_Z....c.G.N.a...?/..%. .- ..K.td....4...5.(.e.`G7..]t?.3..\..... ....G.H...

Chrome Cache Entry: 266

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:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC 14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2Zb3Q&sid=bafhQb8luy6TyutvAC5k
Preview:	2

Chrome Cache Entry: 267

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:	40B244112641DD78DD4F93B6C9190DD46E0099194D5A44257B7EFAD6EF9FF4683DA1EDA0244448CB343AA688F5D3EFD7314DAFE580AC0BCBF115AECA9E8DC 14
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZEp6&sid=bafhQb8luy6TyutvAC5k

Preview:	2

Chrome Cache Entry: 268	
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/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZMuN&sid=bafhQb8Iuy6TyutvAC5k
Preview:	2

Chrome Cache Entry: 269	
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: 270	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (3041), with no line terminators
Category:	downloaded
Size (bytes):	3041
Entropy (8bit):	5.443939715136298
Encrypted:	false
SSDEEP:	48:8/JawL2CDpLGLg0ELdcImwDb3+qoekDYk/GCqpufqv0wgViv9Y+eMNzeRqKb+mpZ:cL5ug3dVf+qpkMkgpufqvFgVi++ecUqK
MD5:	2A29FC3105377608989FDCF710A47554
SHA1:	F6AC20B91A57841A4F84A7DAFA490502FB20D6A4
SHA-256:	8DC4107571BA20983D62DF95A23D5CABC961418C55B75A8CEB1437A83CC7AB3F
SHA-512:	85FFFBC2A8681989E048E9A3E754ADE8D60C9FA603F88747C73C0EC02848EEF34A703EA47F0DCF40B59405B02FBA2C1B3F1700DE8D7710B9DBC6F7291B1EAB5A
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/passwordstrengthmeter.js

Preview:	var PasswordStrengthMeter=function(){function n(n,t,i){(this.PasswordMeterDiv=document.getElementById(n+"_passwordStrengthMeter"),this.PasswordStrengthMeterId=n,this.PasswordTextBox=document.getElementById(t),this.PasswordTextBox!=null)&&(this.PropertySheetId=i,this.PasswordTextBox.PasswordStrengthManager=this,this.PasswordTextBox.onchange=this.TextChangedHandler,this.PasswordTextBox.onkeyup=this.TextChangedHandler,this.PasswordTextBox.PasswordStrengthManager.EvaluatePassword(!1),this.PasswordStrengthMeterDisplayed=!1)}return n.prototype.EvaluatePassword=function(t){var i='weak',r;this.SetMeterLevel(this.PasswordStrengthMeterId,n.METERLEVEL_URGENT),r=this.PasswordTextBox.value,n.ClientSideStrongPassword(r)?(i='strong',this.SetMeterLevel(this.PasswordStrengthMeterId,n.METERLEVEL_HEALTHY)):n.ClientSideMediumPassword(r)?(i='medium',this.SetMeterLevel(this.PasswordStrengthMeterId,n.METERLEVEL_CAUTION)):n.ClientSideWeakPassword(r)&&(i='weak'),this.PasswordMeterDiv.innerText=i,this.PropertyS

Chrome Cache Entry: 271	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	5.281476637177851
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8DHgWdzRiAU2uvxV1JSwULeRSGlslhIRzAg6n:MMHdVBMHgWdzR05cwULeR1D6
MD5:	7FB66B08BBBC3DE1FE114EBB4B666EDC
SHA1:	094D777A647C6C05D8C539E7637ECD91E73D8A34
SHA-256:	55DD88D296E6194AB64EC6D1E2752E80ADE7DD53BA6CE7E9DE91770D81AC7ED6
SHA-512:	D80B5F0165F17104BB0AAB6F4873E6B88A17DD9DA5D672F0AE0A7BCF68BA01083B407B4E2138FF7BAEB76B7CB4F1213A3B781C5B55B19213F5C54A2BC807823A
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/Images/transparent.gif
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>OutOfRangeInput</Code><Message>One of the request inputs is out of range..RequestId:06277f53-901e-0031-7c6f-5b1e84000000.Time:2023-03-20T21:03:35.2936630Z</Message></Error>

Chrome Cache Entry: 272	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.913683277555094
Encrypted:	false
SSDEEP:	3:+WMxvkDotMHUSS1M0YJ8TWEJ/SVxm2TAKQR/xzJxQXQ:+WM5kDotIUznYJOWg/Szm2kRJzLt
MD5:	F7F4BD78815D686F3A3D407925703BFC
SHA1:	96FBF078CB84CC04D78D2B515BED9D1306BAF3CC
SHA-256:	43196ED91EF04D45758F6B36F29EAAE3E8A7F3C0DA1228AE57D8CA75B5A08A7F
SHA-512:	B2C6AE0F5FDC00F58E875DD25259865709D75F4DCF725435730661A0C49F4E9D67C93CCDD26F3F657FE6406F34D8D57C425853D41F9B72095177E4C982579D5
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZDWQ
Preview:	0{"sid":"bafhQb8Iuy6TyutvAC5k","upgrades":["websocket"],"pingInterval":7000,"pingTimeout":15000,"maxPayload":5000000}

Chrome Cache Entry: 273	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5435
Entropy (8bit):	4.729886758075337
Encrypted:	false
SSDEEP:	96:Qf/Or7Vir8P8KJfGVfd+nPkRCrthXXQJ/T6SXuVX3ns9ozR0z5tsQyiPr:q/Okr8P8KBGVUnsCrthHQJb6SXuVnn8v
MD5:	5FEAA482D83C2A69D012F9BFF660D373
SHA1:	EE586D2B46E1A0110C581D507033480A40704606
SHA-256:	356F7D1241F92C9DE9C9CFD0BEBB6C10D1B38508A3F37CEBC26329C656BAD19F
SHA-512:	BC07C9DB3C3494A46E4246CAB6EBE39215F01AE5329A333C2872052992DC1E23765C1826631113F5AC6FC932ED7F17DC5030AB78457D2BFF3E0AA0F7472A4EE2
Malicious:	false
Reputation:	low
URL:	http://https://account.live.com/Resources/images/Microsoft_Logotype_Gray_X-qkgtg8KmnQEvm_9mDTcw2.svg

Preview:	<?xml version="1.0" encoding="utf-8"?>..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... width="47px" height="9px" viewBox="0 0 47 9" xml:space="preserve">..<style type="text/css">....st0{fill:#008A00;}....st1{fill-rule:evenodd;clip-rule:evenodd;fill:#FFFFFF;}....st2{fill-rule:evenodd;clip-rule:evenodd;fill:#008A00;}....st3{fill:#0078D7;}....st4{fill:#094AB2;}....st5{fill-rule:evenodd;clip-rule:evenodd;fill:#094AB2;}....st6{fill:#DC3C00;}....st7{fill-rule:evenodd;clip-rule:evenodd;fill:#DC3C00;}....st8{fill:#107C10;}....st9{fill-rule:evenodd;clip-rule:evenodd;fill:#107C10;}....st10{fill:#D24726;}....st11{fill:#FFB800;}....st12{fill-rule:evenodd;clip-rule:evenodd;fill:#434856;}....st13{fill-rule:evenodd;clip-rule:evenodd;fill:#FFB800;}....st14{fill:#2A3282;}....st15{fill:#249DD1;}....st16{fill:#A0D5EB;}....st17{fill:#FFFFFF;}....st18{fill:#666666;}....st19{fill:#00ADF1;}....st20{fill:#00AFF0;}....st21{fill-r

Chrome Cache Entry: 274

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6805
Entropy (8bit):	5.0695268080762395
Encrypted:	false
SSDEEP:	96:EcnAwv2P7VW0NSlTrMFMFCgjXksPsNA4mWTrY3aGoDf:BAU2zVW0NSdaitIrNf
MD5:	652CC043920DC6F065D26942459CD574
SHA1:	3BB112BC09B852BDC78C814E0F643434EBD47B75
SHA-256:	CFF06C4A63AAE8153E0BB2EC323FADA8AF75B6FD4BD133156BB74555FE6E6AC9
SHA-512:	CF4D7F9425F2EDBD8DA1B8F12CB472CA5AE16DF75206A51D2A08D88B85AC1A91EA444089BD195CC7481D8043F1320B0BBFCAA7006D73DD7B133C37C3329A91F
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/officehub/images/content/images/fluent-background-sources/header-default-desktop-652cc04392.svg
Preview:	<?xml version="1.0" encoding="UTF-8"?>..<svg width="2560px" height="340px" viewBox="0 0 2560 340" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">.. Generator: Sketch 51.2 (57519) - http://www.bohemiancoding.com/sketch -->.. <title>Background_2560px_Transparency and gradient_9.6.18_Ignite</title>.. <desc>Created with Sketch.</desc>.. <defs>.. <linearGradient x1="50%" y1="0%" x2="50%" y2="36.7807904%" id="linearGradient-1">.. <stop stop-color="#F3F2F1" offset="0%"></stop>.. <stop stop-color="#F3F2F1" stop-opacity="0" offset="100%"></stop>.. </linearGradient>.. <rect id="path-2" x="0" y="0" width="2560" height="340"></rect>.. <linearGradient x1="46.43137%" y1="93.8222137%" x2="82.3039269%" y2="0%" id="linearGradient-4">.. <stop stop-color="#EFEDE9" stop-opacity="0.2" offset="0%"></stop>.. <stop stop-color="#FFFFFF" stop-opacity="0.25" offset="100%"></stop>.

Chrome Cache Entry: 275

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	downloaded
Size (bytes):	185
Entropy (8bit):	4.944411584960381
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLtjYWRZLhifA1WoTEiX/fTV7Xn:4ovMwl/m27apP3EGWeiWoTZHTRX
MD5:	F1E39404CE08DB025B79CA484A158156
SHA1:	AF3AFE36774FF101DA946E106B99A2D8DAE172EF
SHA-256:	E0E3DD9B0E0334B3F00A860FC3C262A02E10E662C999E81EB0ACDBDB14548C40
SHA-512:	DC5D8BBE7FFF85D21F976E6E7FBE876BC25B81856B88AB6FFC28E50521329F559553A532E0AA4838720CDEAB46708F82796E7A9A915ACCD784867D4FE2280659
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJuk&sid=bafhQb8luy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":false,"userId":"2","name":null,"hasCustomAvatar":false}]}}].2

Chrome Cache Entry: 276

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD01

Malicious:	false
Reputation:	low
URL:	http://https://account.live.com/Resources/images/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(......................................"P.."""""""""""""""""""""""""""""""""""" ...3 3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""" """""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333 33333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""" """""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333 33333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333""""""""""""""""""""""""""""""""

Chrome Cache Entry: 277	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 47818
Category:	downloaded
Size (bytes):	13919
Entropy (8bit):	7.98572491076564
Encrypted:	false
SSDEEP:	384:8ERkpbIMRpcr3UYREUqWQOpSdWM1GiRBB2Qhi+9Fel:8EubUr3UYEUqWQOdM1NRXcl
MD5:	1631C39AF69D99BFD1AEA7ACB8FBC4FA
SHA1:	7613A14FD31A598E3E2365BC8E529DAAC6FD7A4C
SHA-256:	E7DCAF045B59E7C04E1DF2459273E735FAF28E4F6F6FF7741691CE1ACB857DD5
SHA-512:	EC50A403214158576588C5A3EA395F3D80F41797D59517BE27B05FE680417E5109FCFE04A0983DB0E8D2D4E5114753DCB8CF7C43C429B1CDC35A25E6E7A4C15
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_cfi3giy70wfemn6mr5vbma2.js
Preview:	...........}.r#G..._Q.qL7..!<.D.j....m...`S.IF...Y.@.\Uh6..cv^x...+/...r#.......@J..{=1.".q....'.~7_{.......Q.m....Gw...... ..:.,..(... ..~v.+.cQ.Q....lwV.........[.U`..X....;........+..O8.[.....l.8.. ..^(.........i....+...Ww_..>......?...S...(p.......ufv.........Lx...".oV.W...F"...`*^..((..D.Q............}.4.|....X|..f .HX.u.N.?...L........'.w.....BsL........}&I@.BW8@..@.[.....-.i...;..8].X..%..z. M.n..u..v.;.K.^.;...u=1..@.....XL.......W.V.z..p@.........0.^(.............*WK.j......~S......j..o...2..C..8.\....(.9K.wf/.8?.b~:..$.4.w...>0......Xz.d.....J.[.&*..`.D...n.L...7..~.$B.%.i.........`u}. ..P.{....a{_.+.Y...N..X..%,:.......g..{.m=...u+,.C.up1..W...^p...oa}......@.9V@.X3......+...Y.Fb..[.............UdE..p..B.S.3.wC.........P .s\..G...|~........rf.@.a....\....`.$4c7d..H..a..,i .K..&..O.g.[.....)......8...........I*t...... .Tlk...e..+......-.....e..v.)...zz/..H.!4.-..lc.;.suF..qM.....@.uhO..L....'.lj.v...........y..

Chrome Cache Entry: 278	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 113577
Category:	downloaded
Size (bytes):	35823
Entropy (8bit):	**7.993294075345085**
Encrypted:	**true**
SSDEEP:	768:Y3RHzbfzUh1fLqDf+j2mju93n9N7h8o2ynYKCWX8WgnRgoL1Cp:UbaqDWdC7N7h72y12RL1+
MD5:	957CCAAEC3BBDC8FD4129E2412EDE20C
SHA1:	2528E3E157B4C37E4F4979878822B523AAD7ABD9
SHA-256:	BE496ADE64AD854B0B379A96D5FB7CD96BF7167233021128CB97CCF150197B35
SHA-512:	CBE73F576CBA4D2C55D90A15E53C2F00A8CE21035E54CD05547F0EBAFA5EA88CAB354C90ED6731552A75A1FD36D9CD3A0DC818906FDD91A403E475DA38ED5 A31
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/js/asyncchunk/convergedlogin_pstringcustomizationhelper_c0f2645501c8b52bd96c.js
Preview:	...........{..8.(.....f...,.-.....N6........$.)R&)?.{?..*.I.I.=....L.D.P(..B.P....._[?l.}.....O...z{......g[. ..._.~\|sz..t.R...".fQ...$..t+M..l+J.4[.YP.|k..,..Y......Ze..,.8..(4aqz.U.r.t.]...[o.9...Z4..(...{x_. [IZD!...)Q.!..lk.LY.u......Q..y:+.2....*.....p...m...Y..|4.> ...S5.....h..g.PxB...Y\...X&M....."...<l...}.....D.|.....kr..t.....9.n..8.J.=."a.....[.B..o. A....y..%...cTtr..-W.....by..V,.%.Q..r.lm...l.. {.Uo5..^.......(.U~..?...z.....4].. ...+h.t.o.....{....eu..n=.....e.%..w...X..'..../.....q....wv...._..(..h.e.U.^..$..7...Fc..Z..h.n.....`.NBlV....9_o.l+.z.qs?Y..a..~s....e\|..q.\E.{\|.d,.....nq.J..W. g.\|t...d..8.H5...y^..Y.fn......7.4M....l.c?....!..,....5...p.o!..q.Rc..(.7./iq...:.M..{v..26}u_.. c.:Kj....C......<...D...=[..;c70j/@{\|..B..,.b.4...&....l.Hn.\|.(..d.S6).4/..[D.....(.+.O..U...oi.h.Oc\|. ....65.Z"...)*1Px6.3.B .[P....^.bV.....gHs.J..4.'.\|......-*..Z.Z.W.....\|....7.U.....O+1....c.>.$.'..+.Z'........f....%Tc.o...M.P.+....r.~..g+..

Chrome Cache Entry: 279	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	5.268498969005777
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8DHgWdzRiAU2uvxV1ZL/UiNXKlQzAg6n:MMHdVBMHgWdzR05ZL/Xlx6
MD5:	97AD564BD30EB10D0B9A54A46120CFA8
SHA1:	859556E7967FBDF782298DC6CBFF91FC47B95187

SHA-256:	BF943FFD15608FFA4638BB836BBCE7A556D902B171D955D446B237993125F721
SHA-512:	8769C69444F27ACA0AA81B0E76039B2F14979FF273238AAE0404F4BC46F8CCE16E279D43B04BAFD16BB7FD883CDF21F0412DA2C587BC43AADB6AD12434460BE6
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/Shell/Images/pagelayout_nav_highlight.jpg
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>OutOfRangeInput</Code><Message>One of the request inputs is out of range..RequestId:5e71baf3-201e-001b-056f-5bc194000000.Time:2023-03-20T21:03:34.0480930Z</Message></Error>

Chrome Cache Entry: 280

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	194
Entropy (8bit):	5.014114983792889
Encrypted:	false
SSDEEP:	3:4ovtrKlvFCm/JfQ2gfqKPv3ULWAlHxAQWAXc13TwJQ3UFExGBdxPls2stEtAp6Vn:4ovMwl/m2mX3EADyG3GX1dU
MD5:	F370E30DC1DAB486C60B724AF0F410A9
SHA1:	D4370031DA06A97C28B6ED586F86CF501E856A3A
SHA-256:	D87F086251B8BC81B39E311BBAEC832AA5E56FF24738A59BF0EBA2EE3EAA1231
SHA-512:	2026BA907A22EF38889F6C5451C8E792A58E0465A7387F0080489712764A651AE00143A2E502F2351306DDF6B28767507594CA37E12634FFA050E1852B9312BD
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZadP&sid=bafhQb8luy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USER_CURSOR_CHANGED","response":{"error":null,"data":{"userId":"24404463343","userPosition":{"head":198},"docVersion":10,"docOrSelHasChanged":false}}}]

Chrome Cache Entry: 281

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.2658940075964145
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH1gjGQEFVVKlZLe8g6n:MMHdVBKW/UTqkOo6
MD5:	D550452313010F2E0FEA16A62E7E190A
SHA1:	037F94F9887E4DF9AF65DB8A3550793C19A6C75F
SHA-256:	69906CFF3B373C929439A0BEF991A4A877D7B5B143DF013423A91415505E54A3
SHA-512:	BD9828815EC4408ED00BE722BB8674F8B0FD33813A399AA52998CCA2E7367C333C397342CEB9D17DA04DC35C549A1DE1FE45E078DC7D54935ABFD04F9346789
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/images/scrollbar/arrow_staticdown_16.png
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:d4fbaa2a-e01e-0054-466f-5b8596000000.Time:2023-03-20T21:03:57.8038675Z</Message></Error>

Chrome Cache Entry: 282

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: 283	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.260686566077445
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH1xRGIumdfclZLQDWAg6n:MMHdVBKW/UTBN9uJF6
MD5:	205CFB740EECF41BA0A5C1F306F4C08B
SHA1:	D9AAA9BFE5CF2E0161DDA88D1DD1D3DE248E3783
SHA-256:	E1A3D407F092E3A084BD220C964F4A7545DC6A6795D18C95487832384B768A5C
SHA-512:	370CDA80918D850D8303B3F0B0D2A570E91A60399ED5D8B496627B6D4F8415A2D14819F051D884142BF2880EF97DBA75E430FD9DCF52420FB8B8900973FAB022
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/images/spinner_16x16_metro.gif
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:905a364c-601e-004a-7f6f-5b694e000000.Time:2023-03-20T21:03:57.6567321Z</Message></Error>

Chrome Cache Entry: 284	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	215
Entropy (8bit):	5.333740628066086
Encrypted:	false
SSDEEP:	6:JiMVBdgqZjZWtMfgRTH1ACWJV2VJQeclITrdg6n:MMHdVBZWyUTqVJVUJOS6
MD5:	9C545D2DC9BCC1B7E853723048B49F6B
SHA1:	9A2F2CA10B87FC0741EB6937C559613ADB0DEF6A
SHA-256:	FDC329ED107F4D460E4ED3CB20872B6861DBA3E05C27396A5D00770FF872269E
SHA-512:	138F90104833FBEA78953DD82C7D32D1EC312AEE95EAD9BE23D84B3290BF16BDF05ADC1E5498235FE0A78D38FE8C3F6437197B5688071C114AB0A9DD282D7B 4
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/home.js
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>BlobNotFound</Code><Message>The specified blob does not exist..RequestId:e8269392-d01e-0002-756f-5 b7479000000.Time:2023-03-20T21:03:56.7613645Z</Message></Error>

Chrome Cache Entry: 285	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	downloaded
Size (bytes):	1707
Entropy (8bit):	4.801685421071806
Encrypted:	false
SSDEEP:	24:TEiupF0iupFUhUhUhUdJUhUhUhUhUSUhUhU+1iujzqF2:TEioCioJ1i6r
MD5:	F0AB60B228FA5DB32B87B31A44705812
SHA1:	80EFB558669E49244AC41CF5FE07FD721B670505
SHA-256:	1B4FF455CC186991A57A153B0364E4312779E61995E365E7E98AEBE13AE88334
SHA-512:	D72D3AF455260B9EA6E40084AF0AAD9838A898C634C2D8ABCBFC8A061E5C18056FE90FF473F18D907CFFA3BBCCC5F0EE8053A7F69EE4B8A73EB311427A3BD 6B5
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZCYs&sid=z5Pk-iNyt0hd5jCcAC5e

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},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"13924919","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false,"isExistingCollaborator":true},{

Chrome Cache Entry: 286	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65447)
Category:	downloaded
Size (bytes):	159373
Entropy (8bit):	5.226444625327631
Encrypted:	false
SSDEEP:	1536:WgFAhcPyCrbqhRtFV1l0UBVHyfN+e/KOoF07JWwhmbkxXnFRGvTWlGWLwD3CyY8T:W0SCUbyfMe/KOwNDgxVRGvTgGWCTT
MD5:	B4CD7CF90D9F0EE2D9D5504FEF529244
SHA1:	7EDE840F4CBD9FACB3AD35B552E040FB367DB70C
SHA-256:	41A8EB2356079E81D6A1166D5872E9F4BDF6BAE18699A0A552510CA518FC30B8
SHA-512:	7E8C1CE637B0B484B4BABDD7BC7C61A277306D94F837C92EAAA027248ADDE3E5612113D1D0B4BEEC0D807B6F2F9055E087E486B018F4F8CF45C2967885345 C
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/jsc/angularlib.js
Preview:	/*!. AngularJS v1.3.15. (c) 2010-2014 Google, Inc. http://angularjs.org. License: MIT.*/.(function(n,t,i){'use strict';;function v(n){return function(){for(var i=arguments[0],u,t,r="["+(n?n+":":"")+i+"] http://errors.angularjs.org/1.3.15/"+(n?n+"/":"")+i,i=1;i<arguments.length;i++)r=r+(1==i?"?":"&")+"p"+(i-1)+"=",u=encodeURIComponent,t=arguments[i],t="function"==typeof t?t.toString().replace(/ \{[\s\S]*$/,""):"undefined"==typeof t?"undefined":"string"!=typeof t?JSON.stringify(t):t,r+=u(t);return Error(r)}}function wr(n){if(null==n||vr(n))return!1;var t=n.length;return n.nodeType===at&&t?!0:l(n)||s(n)||0===t||"number"==typeof t&&0<t&&t-1 in n}function r(n,t,i){var u,f,e;if(f(n)if(o(n))for(u in n)"prototype"==u||"length"==u||"name"==u||n.hasOwnProperty&&!n.hasOwnProperty(u)||t.call(i,n[u],u,n);else if(s(n)||wr(n))for(e="object"!=typeof n,u=0,f=n.length;u<f;u++)(e||u in n)&&t.call(i,n[u],u,n);else if(n.forEach&&n.forEach!==r)n.forEach(t,i,n);else for(u in n)n.hasOwnProperty(u)&&t.call(i,n[u

Chrome Cache Entry: 287	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.243936173729868
Encrypted:	false
SSDEEP:	6:JiMVBdgqZj8FWtkwgRTH15tBVgSlZLkg6n:MMHdVBKW/UT5BVg0p6
MD5:	9441E16E2934C54FB27DB60E7DECFB8A
SHA1:	27E9A53D55B5F705732170477D483B1F5F6D0F3D
SHA-256:	F3FE6A1F03BC9EC8366B250AA341C92C01DAF3AA735759063EBE87673B541A51
SHA-512:	908F7E3B573D7D07D2CA870D8BEA6B49C128C4E0EEF5BA4C11CAA118971313D24C4BD84113A245348CD3ABEC1902FBCFF187963D6CFBCD750FC9AF901FAED 21B
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/shell/images/signup_ms_logo.png
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>ResourceNotFound</Code><Message>The specified resource does not exist..RequestId:348ea33a-801e-000f-356f-5bbcad000000.Time:2023-03-20T21:03:57.4411598Z</Message></Error>

Chrome Cache Entry: 288	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (21034), with no line terminators
Category:	downloaded
Size (bytes):	21048
Entropy (8bit):	5.247105700561187
Encrypted:	false
SSDEEP:	192:g3zpKuvV3FObHXVTebI38CI2hpE++Gv30v5z6X/PfGIR2Mh4fZqZXY+iSvkDDx9g:g3lKuvV3FObHXV80DhpnMUAMq6XpJ
MD5:	9EEF535DBB899CD79ED815061D2155E0
SHA1:	F27F009D7B2DD62715CBC725E5405A6B14BD9682
SHA-256:	0FEFA7F702A66FBB2ACD19DB8662D3F0A41D886E8DD45A162455237C80403C26
SHA-512:	E5785105962FAFEF2F92F2FD954A3A4188050BDD3ACEF4E2056986567551E3273CDE8972CE3BA212C3613C83764BD65F8D28AF818EF42C47DEB29D2389700706
Malicious:	false

Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/content/css/signup16.css
Preview:	@font-face{font-family:'SegoeUI-SemiLight-final';src:url('https://res.cdn.office.net/admincenter/admin-content/en/css/webfonts/segoeui-semilight-final.eot');src:url('https://res.cdn.office.net/admincenter/admin-content/en/css/webfonts/segoeui-semilight-final.eot?iefix') format('embedded-opentype'),url('https://res.cdn.office.net/admincenter/admin-content/en/css/webfonts/segoeui-semilight-final.woff') format('woff'),url('https://res.cdn.office.net/admincenter/admin-content/en/css/webfonts/segoeui-semilight-final.ttf') format('truetype'),url('https://res.cdn.office.net/admincenter/admin-pkg/en/css/webfonts/segoeui-semilight-final.svg#web') format('svg');font-style:normal;font-weight:normal}html,body{height:100%}body{font-family:'SegoeUI-Regular-final','Segoe UI','Segoe WP',Tahoma,Arial,sans-serif}.hiddenImportant{display:none!important}.hidden{display:none}a{color:#da3b01;text-decoration:none}a:hover{color:#b22a0f}.container{min-height:100%;height:auto!important;height:100%;margin:0 auto

Chrome Cache Entry: 289	
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/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZPPp&sid=bafhQb8Iuy6TyutvAC5k
Preview:	2

Chrome Cache Entry: 290	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.911046379915681
Encrypted:	false
SSDEEP:	3:4ovtrKIvFCm/JfQ2gHrgGFSwtHv3ULWAlHxPLt4JdZLhifA1WoTEiX/fTVn:4ovMwl/m27apP3EoyiWoTZHTV
MD5:	3A1354A50D4950EA728C84B623B2ECDC
SHA1:	ED0A9680DF4BC76019C6271555228C53AD03F766
SHA-256:	234B4EEF13DFB1C06F63FDE4EE694E71E4A76CD7F26E0206DF0633B4268742D4
SHA-512:	A3CA6CAB5316684CC2CE4DA273B09A52D4F80C1069157B7DD675CE43EFB7978860D6AF70771888ED1E1999FA27C856100CC6B1F458DDFBFB17CD15BC1C2A7CB
Malicious:	false
Reputation:	low
URL:	http://https://notes.services.box.com/3/9159/3001/socket.io/?clientVersion=8.2297.0&EIO=4&transport=polling&t=OS2ZJZ1&sid=bafhQb8Iuy6TyutvAC5k
Preview:	42["message",{"component":"PM_DOC","type":"USERS_CONNECTION_STATUS_CHANGED","response":{"error":null,"data":[{"isConnected":true,"userId":"2","name":null,"hasCustomAvatar":false}]}}]

Chrome Cache Entry: 291	
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:U6OZDyZGokJpZZqOVr4LXQvRn8II2sK5KcF8NcdKP66Po0Nhdh9e0Zup39sDlrG1:U6OZ5nJpZZqY8gvRn9MKlu8N3P6cVhrE
MD5:	5014BD57D455109B69EC9B55F8F846C2
SHA1:	737038FCE3C91AFDBE4EC5E92F9122B66FFA9003
SHA-256:	A35DE03842CE1919D276CDCBEA23ECC2D247932710B92490E08B5BEDE398E28E
SHA-512:	00BA68BB5CDE01C65C03F75AA459F02322F7B6F4E703E9B35BE46EEB4F9FC1F3F051B6A3088E835A8C5840AEB6814673694CC851A70C1DD9221F455327FDEC03
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..\_.@).....$....q...M.:....e.1...bd.K...&..P.i.....`!....[....O. Q_I@.....D._.3.6.v.....9$..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: 292	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	XML 1.0 document, Unicode text, UTF-8 (with BOM) text
Category:	downloaded
Size (bytes):	215
Entropy (8bit):	5.256543005661558
Encrypted:	false
SSDEEP:	3:JLWMNHU8LdgCAqZj+kKlGjoWWUAVMABcyFKBWRTWA1M0IqAtEP9/iWEVemSj/Z3Y:JiMVBdgqZjZWtMfgRTH1u7tDlmAg6n
MD5:	7AE5A50E9F097B44394C7D230FD7CFEE
SHA1:	63D2E949C609B973D9F10041B41EEE13098AA589
SHA-256:	DF7DB4729A52D6BB0305B475B2E1F2C7C49B4BEAFE008AD7F87C795E8CFE0B94
SHA-512:	B56D21429B2043B99CFCFE88C6D9B6603F8D65378F1C372F18E574AF7658203E50DD99EF91415AD2D2FF190BC6E7BC600AF88F2A14CF5EAC70FD8162016F13BA
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/js/webtrendsstream.js
Preview:	.<?xml version="1.0" encoding="utf-8"?><Error><Code>BlobNotFound</Code><Message>The specified blob does not exist..RequestId:2a0de7de-601e-005a-1b6f-5bac26000000.Time:2023-03-20T21:03:56.7701711Z</Message></Error>

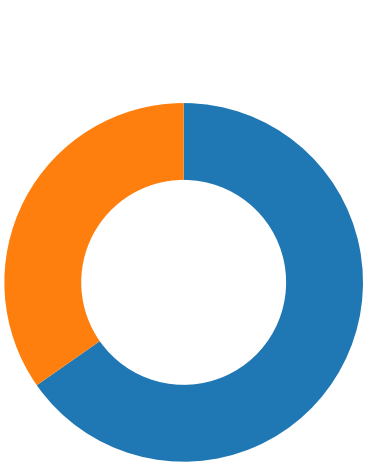
Chrome Cache Entry: 293	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (65533), with no line terminators
Category:	downloaded
Size (bytes):	1314701
Entropy (8bit):	5.192545525675105
Encrypted:	false
SSDEEP:	6144:mZ18TNwHUqPb4QOv3qZ4x8PIQpIhDe6RaHc4Rqt/6QY0ED7PWMtyJk7eOMTu8Q:/TGP/Z7IWy/6QYl6Mt5eOMTu8Q
MD5:	AB16D95569464FDFB578C07A118FD592
SHA1:	CB1FD29405D4F516E545F3D4E5E62930E318DA0C
SHA-256:	4BD97455578BCFF5E1C17656E365A95F69D46B2E0708E61FA71F133D4A1E0A1C
SHA-512:	8AD4A4F634EDFA1D4BCC75551E0A51AE0F3399F3EA4D55845E481CDEFFDE00B8090E2A287940DA66136EF29A2288C879166D45B68555B8E7A3864C3DC57851EC
Malicious:	false
Reputation:	low
URL:	http://https://res.cdn.office.net/admincenter/admin-pkg/2023.3.13.2/en/admin/css/admin.css
Preview:	.fake{color:red}.k-reset{margin:0;padding:0;border:0;outline:0;text-decoration:none;font-size:100%;list-style:none}.k-floatwrap:after,.k-slider-items:after,.k-grid-toolbar:after{content:"";display:block;clear:both;visibility:hidden;height:0;overflow:hidden}.k-floatwrap,.k-slider-items,.k-grid-toolbar{display:inline-block}.k-floatwrap,.k-slider-items,.k-grid-toolbar{display:block}.k-block,.k-button,.k-header,.k-grid-header,.k-toolbar,.k-grouping-header,.k-tooltip,.k-pager-wrap,.k-tabstrip-items .k-item,.k-link.k-state-hover,.k-textbox,.k-textbox:hover,.k-autocomplete,.k-dropdown-wrap,.k-picker-wrap,.k-numeric-wrap,.k-autocomplete.k-state-hover,.k-dropdown-wrap.k-state-hover,.k-picker-wrap.k-state-hover,.k-numeric-wrap.k-state-hover,.k-draghandle{background-repeat:repeat;background-position:0 center}.k-link:hover{text-decoration:none}.k-state-highlight>.k-link{color:inherit}.k-textbox>input,.k-input[type="text"],.k-input[type="number"],.k-textbox,.k-picker-wrap .k-input,.k-button{font-si

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:03:01.550669909 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:01.550729036 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:01.550800085 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:01.551098108 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:01.551147938 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:01.551208019 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:01.552061081 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:01.552081108 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:01.564697027 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:01.564732075 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:01.634155035 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:01.638120890 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:01.644058943 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:01.644114971 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:01.644275904 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:01.644328117 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:01.644961119 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:01.645055056 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:01.645946980 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:01.646004915 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:01.646061897 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:01.646075964 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:03.289802074 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:03.289849043 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.290095091 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.295917034 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:03.295949936 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.341474056 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:03.341519117 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:03.341727972 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:03.341736078 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:03.341814041 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:03.352619886 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.352797031 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:03.352834940 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.353135109 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.353250980 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:03.379600048 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:03.379755974 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:03.379827976 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:03.380004883 CET	443	49701	142.250.203.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:03:03.380105019 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:03.402034998 CET	49701	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:03:03.402084112 CET	443	49701	142.250.203.110	192.168.2.3
Mar 20, 2023 22:03:03.402628899 CET	49700	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:03:03.402674913 CET	443	49700	142.250.203.109	192.168.2.3
Mar 20, 2023 22:03:03.534034967 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.534101009 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.534203053 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.534605026 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.534646034 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.534724951 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.535310030 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.535341978 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.535806894 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.535834074 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.606745005 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.609806061 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.620577097 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.620634079 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.620734930 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.620785952 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.622158051 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.622214079 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.622266054 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.622328043 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.629239082 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.629271030 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.629431009 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.629509926 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.629533052 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.629657984 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.629698992 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.629865885 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.697244883 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.697310925 CET	443	49703	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.797208071 CET	49703	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:03.834733009 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:03.834858894 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.041641951 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.041687965 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.041748047 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.041764975 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.042978048 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.043075085 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.045258045 CET	49702	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.045280933 CET	443	49702	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.191299915 CET	49706	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.191353083 CET	443	49706	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.191456079 CET	49706	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.191847086 CET	49706	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.191860914 CET	443	49706	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.239106894 CET	443	49706	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.239660978 CET	49706	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.239782095 CET	443	49706	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.242291927 CET	443	49706	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.242382050 CET	49706	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.292994976 CET	49706	443	192.168.2.3	74.112.186.144
Mar 20, 2023 22:03:04.293042898 CET	443	49706	74.112.186.144	192.168.2.3
Mar 20, 2023 22:03:04.293262005 CET	49706	443	192.168.2.3	74.112.186.144

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:03:01.389111996 CET	62704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:01.391566992 CET	49977	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:01.409418106 CET	53	62704	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:01.409454107 CET	53	49977	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:02.987932920 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:03.009526968 CET	53	52387	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:04.123784065 CET	53975	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:04.153419018 CET	51139	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:04.176764011 CET	53	51139	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:04.800143003 CET	60582	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:04.819751978 CET	53	60582	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:07.304430008 CET	59636	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:07.308151960 CET	55638	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:07.326113939 CET	53	59636	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:08.015892029 CET	57704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:08.033582926 CET	53	57704	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:29.373085976 CET	61416	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:29.397990942 CET	53	61416	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:31.586025953 CET	59581	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:33.806426048 CET	53428	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:33.824716091 CET	53	53428	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:53.897528887 CET	64121	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:57.577039003 CET	60473	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:57.990288019 CET	56616	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:58.007580996 CET	53	56616	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:58.429322958 CET	61184	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:58.973036051 CET	57387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:58.990860939 CET	53	57387	8.8.8.8	192.168.2.3
Mar 20, 2023 22:03:59.224914074 CET	53269	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:03:59.935606003 CET	62431	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:04:04.851407051 CET	55390	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:04:04.869457006 CET	53	55390	8.8.8.8	192.168.2.3
Mar 20, 2023 22:04:07.005312920 CET	64376	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:04:07.031434059 CET	53	64376	8.8.8.8	192.168.2.3
Mar 20, 2023 22:04:12.946952105 CET	52741	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:04:12.975996017 CET	53	52741	8.8.8.8	192.168.2.3
Mar 20, 2023 22:04:13.129302979 CET	60644	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:05:04.923738956 CET	52365	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:05:04.941706896 CET	53	52365	8.8.8.8	192.168.2.3
Mar 20, 2023 22:05:10.113532066 CET	61937	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:05:10.141859055 CET	53	61937	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 20, 2023 22:03:04.974989891 CET	192.168.2.3	8.8.8.8	d0c3	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:03:01.389111996 CET	192.168.2.3	8.8.8.8	0xa018	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:01.391566992 CET	192.168.2.3	8.8.8.8	0x3840	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:02.987932920 CET	192.168.2.3	8.8.8.8	0x6560	Standard query (0)	nnegri-ubaes.app.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:04.123784065 CET	192.168.2.3	8.8.8.8	0xe6b	Standard query (0)	cdn01.boxcdn.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:03:04.153419018 CET	192.168.2.3	8.8.8.8	0x8b22	Standard query (0)	notes.services.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:04.800143003 CET	192.168.2.3	8.8.8.8	0x3b48	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:07.304430008 CET	192.168.2.3	8.8.8.8	0x96b1	Standard query (0)	client-log.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:07.308151960 CET	192.168.2.3	8.8.8.8	0xf89b	Standard query (0)	sdk.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:08.015892029 CET	192.168.2.3	8.8.8.8	0x3f1a	Standard query (0)	auth.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:29.373085976 CET	192.168.2.3	8.8.8.8	0xa6b1	Standard query (0)	capitaltltleandescrow.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:31.586025953 CET	192.168.2.3	8.8.8.8	0xcb8e	Standard query (0)	identity.nel.measure.office.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:33.806426048 CET	192.168.2.3	8.8.8.8	0xc8e7	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:53.897528887 CET	192.168.2.3	8.8.8.8	0xaa7d	Standard query (0)	portal.microsoftonline.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:57.577039003 CET	192.168.2.3	8.8.8.8	0x69a5	Standard query (0)	www.office.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:57.990288019 CET	192.168.2.3	8.8.8.8	0x7338	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:58.429322958 CET	192.168.2.3	8.8.8.8	0xe479	Standard query (0)	r4.res.office365.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:58.973036051 CET	192.168.2.3	8.8.8.8	0x8a10	Standard query (0)	clientlog.portal.office.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:59.224914074 CET	192.168.2.3	8.8.8.8	0x3c27	Standard query (0)	account.live.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:59.935606003 CET	192.168.2.3	8.8.8.8	0x6c64	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:04.851407051 CET	192.168.2.3	8.8.8.8	0xfc6f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:07.005312920 CET	192.168.2.3	8.8.8.8	0x14af	Standard query (0)	notes.services.box.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:12.946952105 CET	192.168.2.3	8.8.8.8	0xdb38	Standard query (0)	streaming.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:13.129302979 CET	192.168.2.3	8.8.8.8	0xa9c2	Standard query (0)	sdk.split.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:04.923738956 CET	192.168.2.3	8.8.8.8	0x29c4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:10.113532066 CET	192.168.2.3	8.8.8.8	0xc13f	Standard query (0)	notes.services.box.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 22:03:01.409418106 CET	8.8.8.8	192.168.2.3	0xa018	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:01.409454107 CET	8.8.8.8	192.168.2.3	0x3840	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:01.409454107 CET	8.8.8.8	192.168.2.3	0x3840	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.009526968 CET	8.8.8.8	192.168.2.3	0x6560	No error (0)	nnegri-ubaes.app.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:04.146836042 CET	8.8.8.8	192.168.2.3	0xe6b	No error (0)	cdn01.boxcdn.net	cdn01.boxcdn.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:04.176764011 CET	8.8.8.8	192.168.2.3	0x8b22	No error (0)	notes.services.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:04.819751978 CET	8.8.8.8	192.168.2.3	0x3b48	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:07.326113939 CET	8.8.8.8	192.168.2.3	0x96b1	No error (0)	client-log.box.com		74.112.186.144	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 22:03:07.327578068 CET	8.8.8.8	192.168.2.3	0xf89b	No error (0)	sdk.split.io	e3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:08.033582926 CET	8.8.8.8	192.168.2.3	0x3f1a	No error (0)	auth.split.io		44.197.221.236	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:08.033582926 CET	8.8.8.8	192.168.2.3	0x3f1a	No error (0)	auth.split.io		3.223.63.250	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:08.033582926 CET	8.8.8.8	192.168.2.3	0x3f1a	No error (0)	auth.split.io		54.157.194.5	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:08.033582926 CET	8.8.8.8	192.168.2.3	0x3f1a	No error (0)	auth.split.io		35.170.228.5	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:29.397990942 CET	8.8.8.8	192.168.2.3	0xa6b1	No error (0)	capitaltlt leandescrow.net		23.227.196.212	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:31.611857891 CET	8.8.8.8	192.168.2.3	0xcb8e	No error (0)	identity.nel.measure.office.net	nel.measure.office.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:32.229074001 CET	8.8.8.8	192.168.2.3	0xd80b	No error (0)	shed.dual-low.part-0032.t-0009.fdv2-t-msedge.net	part-0032.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:32.229074001 CET	8.8.8.8	192.168.2.3	0xd80b	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.237.60	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:32.229074001 CET	8.8.8.8	192.168.2.3	0xd80b	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.238.60	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:33.824716091 CET	8.8.8.8	192.168.2.3	0xc8e7	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:33.824716091 CET	8.8.8.8	192.168.2.3	0xc8e7	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:53.949503899 CET	8.8.8.8	192.168.2.3	0xaa7d	No error (0)	portal.microsoftonline.com	geo.portal.microsoftonline.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:57.596350908 CET	8.8.8.8	192.168.2.3	0x69a5	No error (0)	www.office.com	home-portal.office.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:57.596350908 CET	8.8.8.8	192.168.2.3	0x69a5	No error (0)	home-portal.office.com	home-office365-com.b-0004.b-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	HHN-efz.ms-acdc.office.com		52.98.241.162	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	HHN-efz.ms-acdc.office.com		40.99.150.66	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	HHN-efz.ms-acdc.office.com		52.98.243.50	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:58.007580996 CET	8.8.8.8	192.168.2.3	0x7338	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.226	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:58.454421043 CET	8.8.8.8	192.168.2.3	0xe479	No error (0)	r4.res.office365.com	r4.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:58.990860939 CET	8.8.8.8	192.168.2.3	0x8a10	Name error (3)	clientlog.portal.office.com	none	none	A (IP address)	IN (0x0001)	false

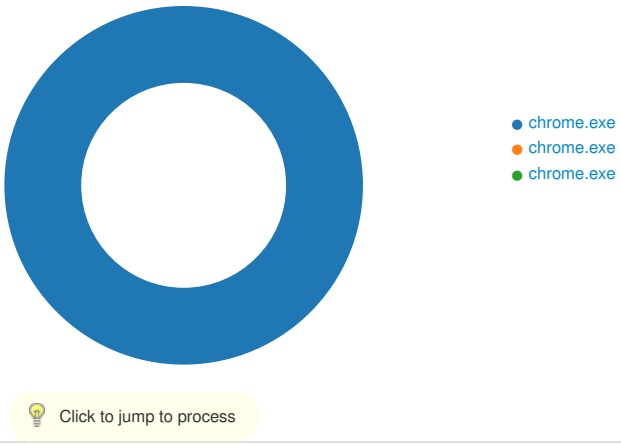
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 22:03:59.242489100 CET	8.8.8.8	192.168.2.3	0x3c27	No error (0)	account.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:59.925420046 CET	8.8.8.8	192.168.2.3	0x1416	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:59.925420046 CET	8.8.8.8	192.168.2.3	0x1416	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:59.956347942 CET	8.8.8.8	192.168.2.3	0xa7b6	No error (0)	shed.dual-low.part-0032.t-0009.fdv2-t-msedge.net	part-0032.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:59.956347942 CET	8.8.8.8	192.168.2.3	0xa7b6	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.237.60	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:59.956347942 CET	8.8.8.8	192.168.2.3	0xa7b6	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.238.60	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:59.966445923 CET	8.8.8.8	192.168.2.3	0x6c64	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:59.966445923 CET	8.8.8.8	192.168.2.3	0x6c64	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:59.966445923 CET	8.8.8.8	192.168.2.3	0x6c64	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:59.983012915 CET	8.8.8.8	192.168.2.3	0xb80c	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:59.983012915 CET	8.8.8.8	192.168.2.3	0xb80c	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:04.869457006 CET	8.8.8.8	192.168.2.3	0xfc6f	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:07.031434059 CET	8.8.8.8	192.168.2.3	0x14af	No error (0)	notes.services.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:12.975996017 CET	8.8.8.8	192.168.2.3	0xdb38	No error (0)	streaming.split.io	split-cname-realtime.ably.io		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:04:12.975996017 CET	8.8.8.8	192.168.2.3	0xdb38	No error (0)	split-cname-realtime.ably.io	dz87sht31vgqa.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:04:12.975996017 CET	8.8.8.8	192.168.2.3	0xdb38	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.9	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:12.975996017 CET	8.8.8.8	192.168.2.3	0xdb38	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.46	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:12.975996017 CET	8.8.8.8	192.168.2.3	0xdb38	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.72	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:12.975996017 CET	8.8.8.8	192.168.2.3	0xdb38	No error (0)	dz87sht31vgqa.cloudfront.net		18.165.183.129	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:13.149106979 CET	8.8.8.8	192.168.2.3	0xa9c2	No error (0)	sdk.split.io	e3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:05:04.941706896 CET	8.8.8.8	192.168.2.3	0x29c4	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:10.141859055 CET	8.8.8.8	192.168.2.3	0xc13f	No error (0)	notes.services.box.com		74.112.186.144	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- nnegri-ubaes.app.box.com
- https:
  - notes.services.box.com
  - client-log.box.com
  - auth.split.io
  - capitaltltleandescrow.net
  - aadcdn.msauth.net
  - outlook.office365.com
  - acctcdn.msauth.net
  - streaming.split.io

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6080**, Parent PID: **2312**

General

Target ID:	0
Start time:	22:02:57
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:	0x7ff614650000
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: **5136**, Parent PID: **6080**

General

Target ID:	1
Start time:	22:02:58
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-US --service-sandbox-type=none --mojo-platform-channel-handle=1828 --field-trial-handle=1820,i,8349816860566181976,962081347468792787 0,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **5544**, Parent PID: **2312**

General

Target ID:	2
Start time:	22:02:59
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://nnegri-ubaes.app.box.com/notes/1169500312889?s=93wior2d16y21cmgyk3biklfy5s0q10w
Imagebase:	0x7ff614650000
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