ID: 358568
Cookbook: browseurl.jbs
Time: 21:06:53
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

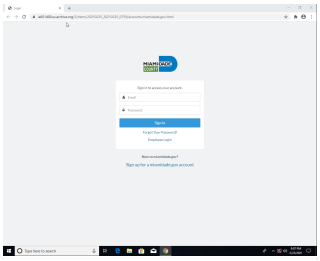
Analysis Report https://ia601400.us.archive.org/3/items/…

Overview

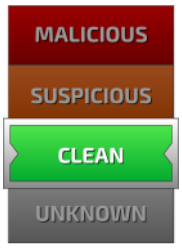
General Information

Sample URL:	http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html
Analysis ID:	358568
Infos:	

Most interesting Screenshot:



Detection

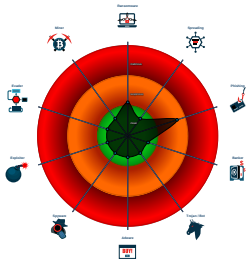


Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Form action URLs do not match mai…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6860 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7124 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1496,7194890310717246147,268159921298456083,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6268 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1496,7194890310717246147,268159921298456083,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3120 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 8164 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1496,7194890310717246147,268159921298456083,131072 --lang=en-GB --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=4288 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

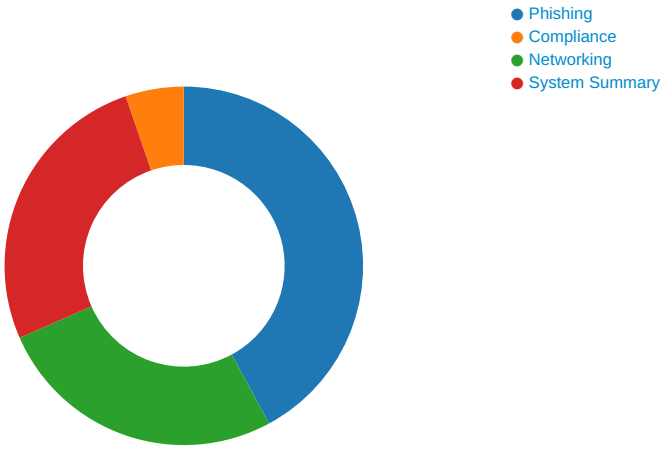
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

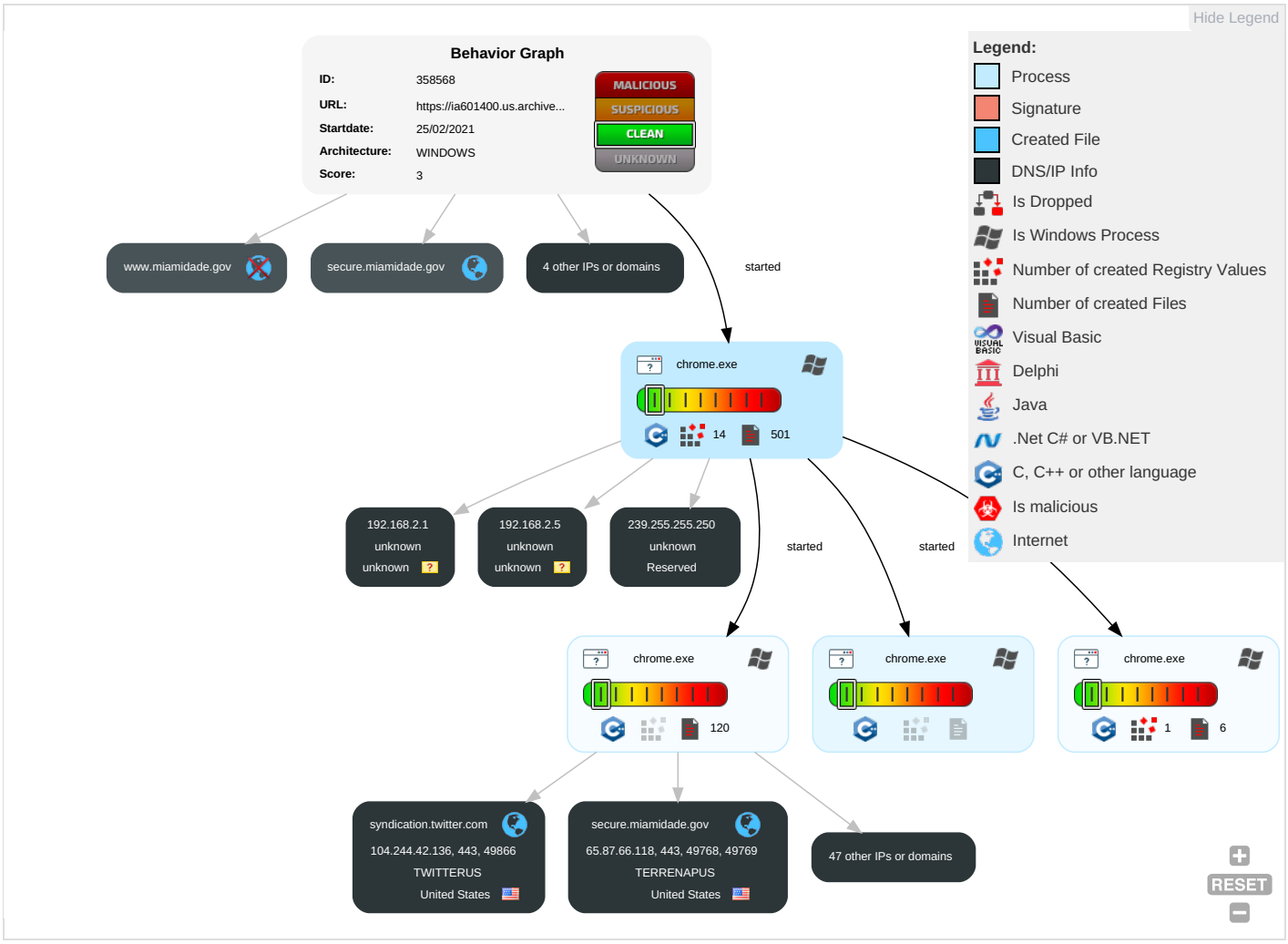
Compliance:

Uses secure TLS version for HTTPS connections

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	I
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

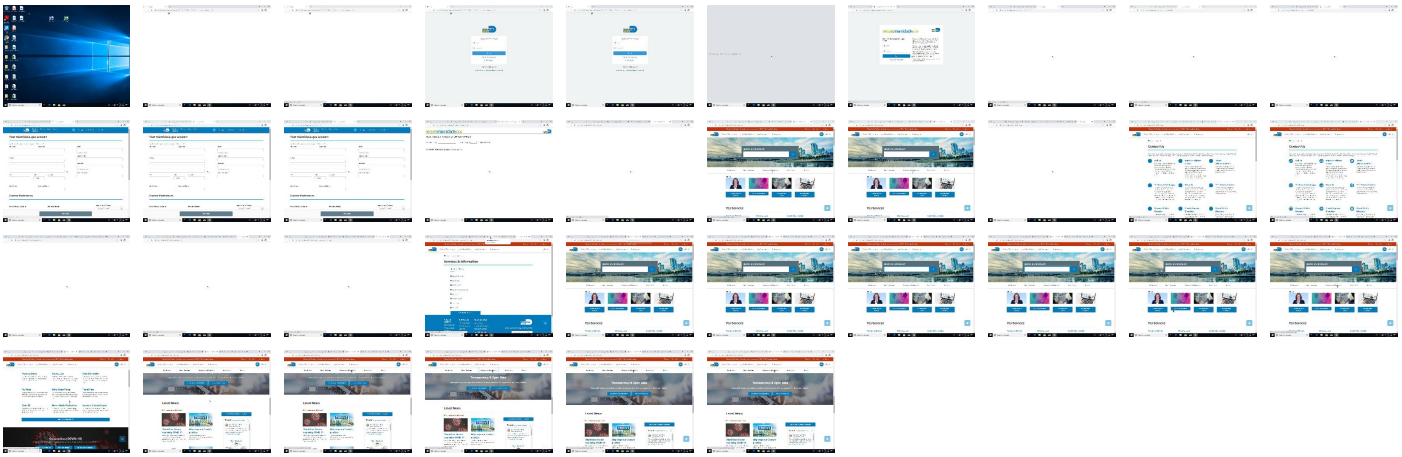
Behavior Graph

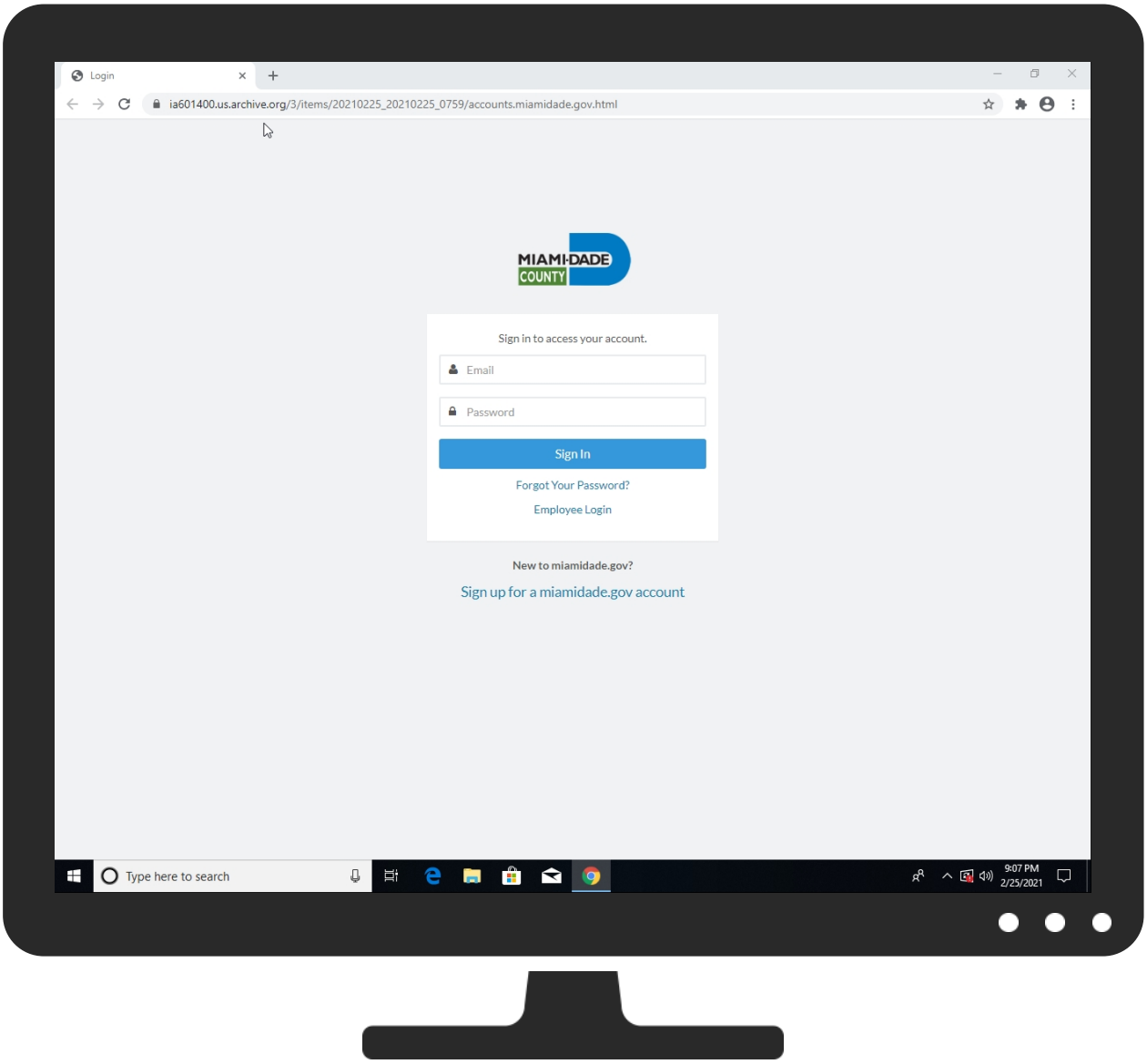


Screenshots

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://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sni1gl.wpc.gammacdn.net	0%	Virustotal		Browse
cdn-backend.levelaccess.net	0%	Virustotal		Browse
www.google.co.uk	0%	Virustotal		Browse
api.levelaccess.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://110005224.collect.igodigital.com/collect.jsaD	0%	Avira URL Cloud	safe	
http://https://110005224.collect.igodigital.com/collect.js	0%	Avira URL Cloud	safe	
http://https://cdn.levelaccess.net/accessjs/YW1wMTI1NzY/access.js	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.miamidade.gov	65.87.66.88	true	false		high
ia601400.us.archive.org	207.241.227.120	true	false		high
sni1gl.wpc.gammacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	74.125.71.154	true	false		high
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
i.ytimg.com	142.250.180.150	true	false		high
nova-collector-1192479543.us-east-1.elb.amazonaws.com	3.221.235.248	true	false		high
cdn-backend.levelaccess.net	13.224.94.91	true	false	• 0%, Virustotal, Browse	unknown
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
syndication.twitter.com	104.244.42.136	true	false		high
secure.miamidade.gov	65.87.66.118	true	false		high
googleads.g.doubleclick.net	216.58.208.130	true	false		high
cs511.wpc.edgecastcdn.net	152.199.21.140	true	false		high
la-pr-analy-1p2sxho81cjid-1195857617.us-east-1.elb.amazonaws.com	52.0.123.75	true	false		high
www.google.co.uk	142.250.184.67	true	false	• 0%, Virustotal, Browse	unknown
photos-ugc.l.googleusercontent.com	142.250.186.33	true	false		high
googlehosted.l.googleusercontent.com	142.250.184.33	true	false		high
miamidade.gov	65.87.66.84	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
siteintercept.qualtrics.com	unknown	unknown	false		high
zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
www.miamidade.gov	unknown	unknown	false		high
cdn.syndication.twimg.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
ton.twimg.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
api.levelaccess.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
static.doubleclick.net	unknown	unknown	false		high
cdn.levelaccess.net	unknown	unknown	false		unknown
dc.services.visualstudio.com	unknown	unknown	false		high
nova.collect.igodigital.com	unknown	unknown	false		unknown
110005224.collect.igodigital.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.miamidade.gov/global/navigation/service-index.page	false		high
http://https://accounts.miamidade.gov/myaccount/	false		high
http://https://www.miamidade.gov/global/home.page	false		high

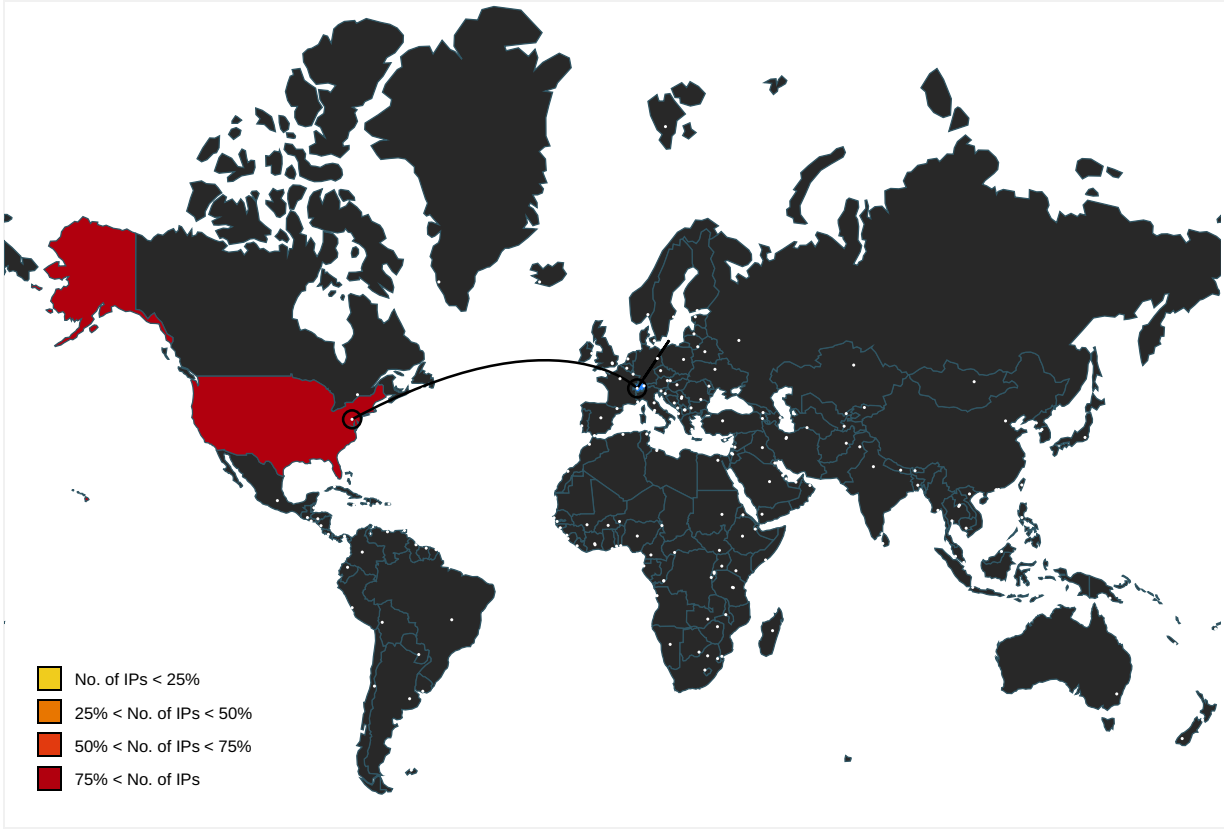
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.miamidade.gov/resources/js/1.8.2.jquery.min.js	fd522d844ad456a7_0.0.dr, 1696134080d701e5_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/angular-moment.min.jsaD	6c4b0316c37cc61f_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/materialize.min.js	e2558cda5ab2a50a_0.0.dr, f65fd237a4111560_0.0.dr	false		high
http://https://110005224.collect.igodigital.com/collect.jsaD	75b95c050691983b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://miamidade.gov/i	a97a76e114b8de08_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/angular.min.js	ccd565be91b80e4c_0.0.dr, 249b940bf2b83f19_0.0.dr	false		high
http://https://www.miamidade.gov/global/navigation/service-index.page	Current Session.0.dr, Favicons.0.dr	false		high
http://https://accounts.miamidade.gov/myaccount/index.html	Current Session.0.dr	false		high
http://https://miamidade.gov/xKy	c72bfd6a7a15adce_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/angular-materialize.min.js	2bc0575a58a7bdad_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/purl.js	aff0ca205d48d930_0.0.dr	false		high
http://https://www.miamidade.gov/	000003.log0.0.dr	false		high
http://https://110005224.collect.igodigital.com/collect.js	75b95c050691983b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.miamidade.gov/resources/js/1.8.2.jquery.min.jsaD	fd522d844ad456a7_0.0.dr	false		high
http://https://miamidade.gov/~	30a737d3a69dec13_0.0.dr	false		high
http://https://cdn.levelaccess.net/accessjs/YW1wMTI1NzY/access.js	b236d738ed517a04_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://miamidade.gov/x	1a99875434b2d16a_0.0.dr	false		high
http://https://miamidade.gov/i2	45324813144077fe_0.0.dr	false		high
http://https://www.miamidade.gov/global/311.pageContact	History-journal.0.dr	false		high
http://https://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/embed.js	1ac412f89d4b472c_0.0.dr	false		high
http://https://youtube.com/BY	335e69ddec2b9ac6_0.0.dr	false		high
http://https://miamidade.gov/o	58f3e4ae2e487b2e_0.0.dr	false		high
http://https://emissive-slates.000webhostapp.com/deller.php	Current Session.0.dr	false		high
http://https://www.youtube.com	000003.log6.0.dr	false		high
http://https://secure.miamidade.gov/favicon.ico	Favicons-journal.0.dr	false		high
http://https://www.miamidade.gov/global/navigation/service-index.pageServices	History-journal.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html	Current Session.0.dr, History-journal.0.dr	false		high
http://https://miamidade.gov/J	f34b2e8dc90cf520_0.0.dr	false		high
http://https://miamidade.gov/C	745493bd88fa4cd1_0.0.dr	false		high
http://https://github.com/urish/angular-moment	6c4b0316c37cc61f_0.0.dr	false		high
http://https://platform.twitter.com/js/timeline.217a220423d55b36c29099c89d1abb2d.jsaD	1a99875434b2d16a_0.0.dr	false		high
http://https://www.miamidade.gov/global/service-list.pageServices	History-journal.0.dr	false		high
http://https://www.miamidade.gov/resources/js/1.4.1.jquery.cookie.min.jsaD	09aa4b2a50563c7a_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/angular-sanitize.min.js	4ef1b04a94f9eaab_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/angular-materialize.min.jsaD	2bc0575a58a7bdad_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/angular.js	49ba72fa34b11a97_0.0.dr, 641c3cccf0e1412f_0.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.htmli	Favicons-journal.0.dr	false		high
http://https://www.miamidade.gov/images/err-logo.gifr	Favicons-journal.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.htmlr	Favicons-journal.0.dr	false		high
http://https://www.miamidade.gov/resources/js/materialize.min.jsaD	f65fd237a4111560_0.0.dr	false		high
http://https://miamidade.gov/U	04c791db684b9b0e_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/moment.min.jsa	12bf4d173f54450b_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://youtube.com/	a11aead48addff6a_0.0.dr	false		high
http://https://www.miamidade.gov/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js	04c791db684b9b0e_0.0.dr	false		high
http://https://secure.miamidade.gov/myemployee/home.page	Current Session.0.dr	false		high
http://https://miamidade.gov/	167b0645db408709_0.0.dr, 2c4c7b900e92b883_0.0.dr, 510f12c38eaabfa6_0.0.dr, 3ee130f137310dbc_0.0.dr, cb14c999099d7751_0.0.dr	false		high
http://https://platform.twitter.com/widgets.jsaD	e946605729594cd4_0.0.dr	false		high
http://https://dns.google	035ee2e4-7d44-462d-96d2-d53ce4147c16.tmp.1.dr, 52a0d3a5-97c7-48e5-b80d-b40f82446b65.tmp.1.dr, a6f627e4-dd09-4d5a-a1fd-4e22f45d4a30.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://momentjs.com/guides/#/warnings/zone/	12bf4d173f54450b_0.0.dr	false		high
http://https://www.youtube.com/ytscframe	Current Session.0.dr	false		high
http://https://platform.twitter.com/js/timeline.217a220423d55b36c29099c89d1abb2d.jsa	1a99875434b2d16a_0.0.dr	false		high
http://https://platform.twitter.com/jot.html	e946605729594cd4_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/dirPagination.jsaD	51828aa6d63df8ef_0.0.dr	false		high
http://https://www.youtube.com/s/player/392133a3/fetch-polyfill.vflset/fetch-polyfill.js	a11aead48addff6a_0.0.dr	false		high
http://https://www.miamidade.gov/global/service-list.page	Current Session.0.dr, History.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/950153867/?random=1614283712003&cv=	3cc37ae85ca32abc_0.0.dr	false		high
http://https://youtube.com/f	5b637dfbcd038651_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/md-global.jsaD	07224a0d300bf0c3_0.0.dr	false		high
http://https://www.miamidade.gov/resources/components/search-index/js/runtime-es2015.0811dcefd377500b5b1a.j	1b04f6e67c0df3da_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/flexMenu.min.js	3be85e22793a2261_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/global-scripts.jsa	429ebb45cfc87783_0.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.htmlF	Favicons-journal.0.dr	false		high
http://https://www.miamidade.gov/resources/js/moment.min.jsaD	12bf4d173f54450b_0.0.dr	false		high
http://https://youtube.com/L	f762371b8dff6236_0.0.dr	false		high
http://https://accounts.miamidade.gov/myaccount/index.htmlUser	History-journal.0.dr	false		high
http://https://www.miamidade.gov/global/navigation/global-search.page	Current Session.0.dr	false		high
http://https://www.youtube.com/	Network Action Predictor-journal.0.dr, 000003.log0.0.dr	false		high
http://https://cct.google/taggy/agent.js	b236d738ed517a04_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/base.js	0fb33271053e6b85_0.0.dr	false		high
http://https://miamidade.gov/ZTc	3be85e22793a2261_0.0.dr	false		high
http://https://miamidadecounty.co1.qualtrics.com/jfe/form/SV_89btbX8j8qKoGfX	b236d738ed517a04_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/950153867/?random=1614283694935&cv=	a97a76e114b8de08_0.0.dr	false		high
http://https://www.miamidade.gov/resources/js/dirPagination.js	51828aa6d63df8ef_0.0.dr	false		high
http://https://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/embed.jsaD	1ac412f89d4b472c_0.0.dr	false		high
http://https://www.miamidade.gov/favicon.ico8	Favicons.0.dr	false		high
http://https://secure.miamidade.gov/myemployee/home.pageEmployee	History-journal.0.dr	false		high
http://https://accounts.miamidade.gov/myaccount/registrationUser	History-journal.0.dr	false		high
http://https://zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com/WRSiteInterceptEngine/?Q_ZID=Z	1aab6f08cdf296e9_0.0.dr	false		high
http://https://secure.miamidade.gov/ERDAdmin/enet/pwdchg.do	Current Session.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.miamidade.gov/ERDAdmin/enet/pwdchg.jspMiami-Dade	History-journal.0.dr	false		high
http://https://www.miamidade.gov/favicon.ico	Favicons.0.dr	false		high
http://https://accounts.miamidade.gov/myaccount/favicon.ico	Favicons-journal.0.dr	false		high
http://https://www.miamidade.gov/resources/js/jquery.url.jsaD	ce25228ae7601a16_0.0.dr	false		high
http://https://www.miamidade.gov/resources/components/search-index/js/main-es2015.a417ee09c81b9425955e.js	510f12c38eaabfa6_0.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html2	History Provider Cache.0.dr	false		high
http://https://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/remote.jsaD	9fecb852ea738613_0.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html3	History-journal.0.dr	false		high
http://https://syndication.twitter.com/i/jot	e946605729594cd4_0.0.dr	false		high
http://https://www.miamidade.gov/images/err-logo.gif	Favicons-journal.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://platform.twitter.com/embed	e946605729594cd4_0.0.dr	false		high
http://momentjs.com/guides/#/warnings/min-max/	12bf4d173f54450b_0.0.dr	false		high
http://https://platform.twitter.com/widgets/widget_iframe.6e189c4f2b6d88c453045806323cdcf3.html?origin=http	Current Session.0.dr	false		high
http://https://www.miamidade.gov/resources/js/flexMenu.min.jsaD	3be85e22793a2261_0.0.dr	false		high
http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.htmlLogin/	History-journal.0.dr	false		high
http://https://www.miamidade.gov/resources/js/global-scripts.jsaD	429ebb45cfc87783_0.0.dr	false		high
http://https://secure.miamidade.gov/	Network Action Predictor-journal.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.184.220.66	unknown	European Union		15133	EDGECASTUS	false
65.87.66.88	unknown	United States		23148	TERRENAPUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.87.66.84	unknown	United States		23148	TERRENAPUS	false
13.224.94.91	unknown	United States		16509	AMAZON-02US	false
142.250.186.33	unknown	United States		15169	GOOGLEUS	false
104.244.42.136	unknown	United States		13414	TWITTERUS	false
3.221.235.248	unknown	United States		14618	AMAZON-AESUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.21.175	unknown	United States		15133	EDGECASTUS	false
65.87.66.118	unknown	United States		23148	TERRENAPUS	false
142.250.184.67	unknown	United States		15169	GOOGLEUS	false
52.0.123.75	unknown	United States		14618	AMAZON-AESUS	false
3.213.223.157	unknown	United States		14618	AMAZON-AESUS	false
74.125.71.154	unknown	United States		15169	GOOGLEUS	false
207.241.227.120	unknown	United States		7941	INTERNET-ARCHIVEUS	false
152.199.21.140	unknown	United States		15133	EDGECASTUS	false
142.250.184.33	unknown	United States		15169	GOOGLEUS	false
216.58.208.130	unknown	United States		15169	GOOGLEUS	false
142.250.180.150	unknown	United States		15169	GOOGLEUS	false
93.184.220.70	unknown	European Union		15133	EDGECASTUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358568
Start date:	25.02.2021
Start time:	21:06:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean3.win@48/249@33/23

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://secure.miamidade.gov/myemployee/home.page • Browse: https://accounts.miamidade.gov/myaccount/registration • Browse: https://secure.miamidade.gov/ERDAdmin/enet/pwdchg.jsp • Browse: https://www.miamidade.gov/global/home.page • Browse: https://www.miamidade.gov/global/311.page • Browse: https://www.miamidade.gov/global/service-list.page
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.64.90.137, 142.250.180.77, 216.58.208.142, 216.58.205.78, 209.197.3.15, 209.197.3.24, 216.58.208.170, 74.125.173.39, 2.20.142.210, 2.20.142.209, 142.250.74.195, 104.43.193.48, 142.250.180.163, 216.58.205.74, 104.19.248.34, 104.19.249.34, 13.88.21.125, 142.250.180.74, 142.250.180.106, 142.250.180.138, 142.250.180.170, 216.58.209.42, 142.250.184.42, 142.250.184.74, 142.250.184.104, 93.184.220.29, 204.79.197.222, 142.250.186.78, 216.58.206.34, 216.58.206.36, 51.11.168.160, 52.147.198.201, 216.58.208.174, 142.250.180.174, 216.58.209.46, 142.250.184.46, 142.250.184.78, 216.58.198.14, 172.217.21.78, 142.250.180.110, 142.250.180.142, 216.58.198.10, 216.58.208.163, 142.250.185.166, 104.17.209.240, 104.17.208.240, 93.184.221.240, 216.58.208.131, 92.122.213.194, 92.122.213.247, 52.155.217.156, 173.194.188.6, 20.54.26.129, 51.107.59.180, 74.125.11.7, 51.104.144.132, 173.194.164.139, 173.194.163.75, 173.194.187.103 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fp.msedge.net, cds.s5x3j6q5.hwcdn.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, clientservices.googleapis.com, r5.sn-4g5e6nle.gvt1.com, r2.sn-4g5e6nsr.gvt1.com, a-0019.a-msedge.net, r1---sn-4g5e6nlk.gvt1.com, clients2.google.com, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, content-autofill.googleapis.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, swn-breeziest-in.cloudapp.net, www.googleapis.com, r2---sn-4g5e6nsr.gvt1.com, skypedataprdcolcus15.cloudapp.net, az416426.vo.msecnd.net, ris.api.iris.microsoft.com, youtube-ui.l.google.com, www3.l.google.com, translate.googleapis.com, blobcollector.events.data.trafficmanager.net, wac.apr-8315.edgecastdns.net, clients.l.google.com, au.download.windowsupdate.com.edgesuite.net, cs2-wac.apr-8315.edgecastdns.net, www.googleadservices.com, r1---sn-4g5edns7.gvt1.com, r5---sn-4g5ednls.gvt1.com, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, redirector.gvt1.com, www.googletagmanager.com, cs11.wpc.v0cdn.net, r1---sn-4g5edne7.gvt1.com, 1.perf.msedge.net, r5.sn-4g5ednls.gvt1.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, www-googletagmanager.l.google.com, wu.ec.azureedge.net, r1.sn-4g5edns7.gvt1.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net,

r1.sn-4g5e6nlk.gvt1.com, static-doubleclick-net.l.google.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net, dc.trafficmanager.net, r1.sn-4g5edne7.gvt1.com, translate.google.com, dc.applicationinsights.microsoft.com, cds.j3z9t3p6.hwcdn.net, r5---sn-4g5e6nle.gvt1.com, www.miamidade.gov.cdn.cloudflare.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:07:40	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	118268

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDf5695NkJMM0/7laXXHAQHQaYfwZ:RN7MlanAQwEIztTmN7MlanAQwEIztTk
MD5:	07E57ED8F424B6844043384CEB8C02CE
SHA1:	4C651F642CEB41785F5E9F5E17A0CCCE6949F8BD
SHA-256:	E8AC8D93636D33F60C7D99AA2A5455EAB4A0F9CBC67A897BBE1FC3EAB6DBF28A
SHA-512:	3F9CBFF0384DD2409D5CB861327C227ADE023D8F65FA2665E87BF435649A613436EB4C37813CF830A32E623AECB417543D81C052A2B00E411587D0AAB3AB248A
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	656
Entropy (8bit):	3.095799064292632
Encrypted:	false
SSDEEP:	12:k3kPlE99SNxAhUeo+aKxha3kPlE99SNxAhUeo+aKt:2kPcUQUj+aKxCkPcUQUj+aKt
MD5:	F69239AD65133C35802EEA85A971093B
SHA1:	AA42F463E17E4B15F1C45D42E1FF7CB2350E1159
SHA-256:	60C06889133C2D2C5740FBB66D0C8B83C6FC9FD0421B4E40606F416D2638520E
SHA-512:	2016F8D38E98B1F2D62C512CF91410893C9DE46965CAFF8678AD76117B52657043EF9CF1557E4A16FF91A581C8D3BC17F2051F5BEEB7BFC2256EAEFC22BC45C
Malicious:	false
Reputation:	low
Preview:	p..... .....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...p..... .....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0545cb1c-6dd2-4b80-b1cc-abb516ac04ec.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7464020381842027
Encrypted:	false
SSDEEP:	384:56wyth/Q6bAX3VcCR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgUegfBtZ6OnnN:8ySSFFizsasenRv383rW/KFjBhF
MD5:	AE97A1601714AC69232627B325395442
SHA1:	699673C0E6835949DFAAFC6EC7DE99CB9D7922A6
SHA-256:	B9D46A799C90130588A5C5A492FB17AB4F6B2150B58C3F5E72F3D7E1757A3294
SHA-512:	623CE554ED5EC09275FF19650AAB0F0DCC43A6C49A6B75862A5F8C95845D3FBD085A86F558D33E88534F28ED79D2B2AFB06E6EC9C182DBE3FF43A6C05D4948D
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\182552fe-d3fb-4cdc-8015-8ed350291e9e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	156941
Entropy (8bit):	6.052620669636947
Encrypted:	false
SSDEEP:	3072:IsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnMFcbXafIB0u1GOJmA3iuRC:vflkhsXNZswa2baaqfIlUOoSiuRC
MD5:	B348C1F2FDAF315F82DC9FE8F1733A23
SHA1:	FBCB65FF10562FC5A25D42834233C6DE9B2D6808

C:\Users\user\AppData\Local\Google\Chrome\User Data\182552fe-d3fb-4cdc-8015-8ed350291e9e.tmp	
SHA-256:	06F690CE16B7B4C4EA058868879576269ED2E6F8EC12E9FDE31E5F9BCD11676C
SHA-512:	4424F01C69A57E3D78937C440D03AB13ECBB27FBF66846203A6A23568004958419F78B7DFF594E73EE38F8A1F534BAE140A5C78A2CF5DCE2EFB5BA19A4B1638
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614283659759702e+12,"network":1.614283662e+12,"ticks":301192148.0,"uncertainty":4570053.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxA AAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Os h5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2P KkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":

C:\Users\user\AppData\Local\Google\Chrome\User Data\26d97f7a-0189-4f5f-8ed9-576f3ff73b99.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	156606
Entropy (8bit):	6.051630337695746
Encrypted:	false
SSDEEP:	3072:hsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnMFcbXafIB0u1GOJmA3iuRC:EflkhsXNZswa2baaqfllUOoSiuRC
MD5:	F3010BA8440BFD7B5CB5B59F6A00E48A
SHA1:	A9D1C7931F104740F38115A078F15B242FBF4117
SHA-256:	B66211A1F24A10F7E8B685D8782C765E43B453716CCA07B6809BE17857345A54
SHA-512:	5953AE5D32402FD15E6697495F9B902A1EF3DBC9662A95C9A77F70DB9B334580E484AB546B4491A648AE7D1B5D5C8CF9051B85C5A5BC1339BE01343CDBB70BF 7
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614283659759702e+12,"network":1.614283662e+12,"ticks":301192148.0,"uncertainty":4570053.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715968761"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\36f7b19e-906a-42b6-a7a4-7fd1abf127d3.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	156606
Entropy (8bit):	6.051629067073289
Encrypted:	false
SSDEEP:	3072:RsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnMFcbXafIB0u1GOJmA3iuRC:0flkhsXNZswa2baaqfllUOoSiuRC
MD5:	A9F844D87262C53A94B4E4BBCED4BA0E
SHA1:	134870C9DD958A73D3428ACDA14B86CFE67B52CB
SHA-256:	00628997E900EF282E96638F477FDF36BC21C717C6E5C2188127367CAC54A78D
SHA-512:	E735006204EDE1DD2A7B9F0D16BD4C4CAE7675B7AE33E16F7A15A9C553A07305C1345785151354FE14B3775D24BB71EB2882D0F5E58CCEFECB3A62EF274F68 F
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614283659759702e+12,"network":1.614283662e+12,"ticks":301192148.0,"uncertainty":4570053.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715968761"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\3fb4c347-a124-46ed-b4d6-5b5ba04a86d8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	165086
Entropy (8bit):	6.081978232088691
Encrypted:	false
SSDEEP:	3072:SGSsmGflW7LtsevCLxZJasImhjp3qm4JaPlrnMFcbXafIB0u1GOJmA3iuRC:nlflkhsXNZswa2baaqfllUOoSiuRC
MD5:	0852F35D24E34DD1669B73383BDBF2F6
SHA1:	0F5A863D2221642288C39DF3C4B0DDA9CB5B3A60

C:\Users\user\AppData\Local\Google\Chrome\User Data\3fb4c347-a124-46ed-b4d6-5b5ba04a86d8.tmp	
SHA-256:	685C59797577F6065D238CCEA367B130989E2F67936465CBA294D1EC84D3ABD4
SHA-512:	6771FEBAE83332C2E9162F5EDC3F52F9BB7F804D4660FA3EB74702EBE59695F4FFE8F8D2B2C40A20BA285969CA0844AC4DEDB3DDD91BD25DC0E4FEA5003374 69
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.614283659759702e+12,"network":1.614283662e+12,"ticks":301192148.0,"uncertainty":4570053.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\81f645b2-4358-4c3e-90df-1fa632c4695e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.747010542299055
Encrypted:	false
SSDEEP:	384:J6wyth/Q6bAX3VcCR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgbgfBtZ6Onntq:sySSFFizOasenRv383rW/KFjBhI
MD5:	2671017EA08B19844D40088036660A11
SHA1:	3E51407511D3FF1A4B339B061EC5B8B704270826
SHA-256:	48748D7D6078994E6EDF8768236568C6B0B8C48D4BAE9ACB52AD707DFC35C2CE
SHA-512:	CD6A9FF8606C5225E50CD4862C5FCB7436E2077B1FD0A0634CDD50AF9F9C028826C8D7C89195CD1F48EA278C0AF1053799849E734FAA6033D6269DC49BDED8
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\8aebfbbd-9477-4b08-9d06-00863f8b0bf8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.746336758954295
Encrypted:	false
SSDEEP:	384:f6wyth/Q6HXwR8NhrqvF/3GJfmHnCGSVrAjtJxeDrbKrolmgbgfBtZ6OnntNE1Js:ynSFFizOasenRv383rW/KFjBhT
MD5:	F10A35ABBFCC93B94B6A9B7CA5CB9B51
SHA1:	1531DCCE9D83A5E7D01A6DDDACFE094BC79ADE1B
SHA-256:	22DDFD3E5D0C89B5869D7A52A4AD784D11F24712FA9BB8A73FF6FD62844A7B37
SHA-512:	CE0BB81384C908EFE52A6F4F3EFD57895DA90A277A5E9F6AD3FE68BEE246B56EB5CADEF83DF77D5CFCB450659B916862DEE1AF015B5F2A6A830E8C1A34C40 2F
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....28.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C5 9
Malicious:	false
Reputation:	low
Preview:	sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\035ee2e4-7d44-462d-96d2-d53ce4147c16.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0748f592-982b-4660-8271-d5d9fc60f101.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5114
Entropy (8bit):	4.961848902195692
Encrypted:	false
SSDEEP:	48:YcYkMklilBqAORqTlYGlQuoTw0xrN4MqM8C1Nfct/9BhUJo3KhmeSnpugkOIJb5t:nWwt4pIVN5k0JCKL8ugkOI1tbOTlVuHn
MD5:	0F3FC9840126F3E6250BBFAAB8556701
SHA1:	4B7680998C91A56BA783B0CFCC3EA31FC9EFAC09
SHA-256:	73746ACEBE0D3360D4EF98621B153B3B88637329FBE2068E05379A7077F0E476
SHA-512:	03FD27173B5E8F796F2C5297715D5E5027B0AFA7361BC098B1F3CE4BFE8F64BAE63C2D70A82396DFB8B9AA3DA456B5E46CD1CB8A3BCFF03A24351E919B91D4 0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258757257241708","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\31cf90e4-5c1e-4a78-99cb-2510708090f7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5711
Entropy (8bit):	5.173328301919349
Encrypted:	false
SSDEEP:	96:nWJE4CRIVZ5k0JCKL8ugkOI1tbOTlVuHn:nW+4CRIzh4KZgkOI9
MD5:	70AE2A6ADA2BFDE6328B82988179F0C9
SHA1:	B0B2491227CB101C8B9F207E28000611EE6126B9
SHA-256:	71964C2048EF71F583D98BAE56834EEBE3900F26278D12500BEED45C96E42C1B
SHA-512:	E4DE623B767CC67ED1C2C6EA7C6A714827B7E4EDA5A147B88D7418EA0F07D2915A3B25714040B8BE1578DFFB6A6E8BB0BB5815EC33148225B73651F407DBB2 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\31cf90e4-5c1e-4a78-99cb-2510708090f7.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258757257241708","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\32c2e418-d717-4915-b9a0-638ed9510a86.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\36a02be1-c1ba-4cff-b835-03287097ab9b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22620
Entropy (8bit):	5.536141226750838
Encrypted:	false
SSDEEP:	384:PP7t7Ll3hXZ1kXqKf/pUZNCgVLH2HfDwrU1HG5nZ27qRJ64I1:5LlVZ1kXqKf/pUZNCgVLH2Hf0rUJG5ns
MD5:	E1336E1775647D44469DA6DC426D101A
SHA1:	B8C5DC383F908511802C48D8201F194B1D42F807
SHA-256:	BCF063B2DD76EC926C1B0DC460F6777555EB3B164258AA58C40C4C6D26282B8C
SHA-512:	2273BAEDC072A8AD66F7B186A3407C259978F9B90D072999A086D39D87F11E65611C4CF61FF7871A00A4733EAC42FFE8CBC57C411E094EFBB1416C70A0D901C
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13258757256981609","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\400835a9-cc7f-49eb-ad83-2afe43e1d9c8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2210
Entropy (8bit):	5.587254932934416
Encrypted:	false
SSDEEP:	48:YQUgvA3wU6eUYNieUR6UUh+UDUIQtSU4cKUaqqPeUekUe1wU03UeP:xU+U6eUOieUoUUMUDUf0U4cKUaRPeU3y
MD5:	E51A1C5159818CF6BC60789356207773
SHA1:	4902392003169B162E2D1452B2D83FD2435D6481
SHA-256:	ACA4D7BBE529F07B1FDE5007B9730260C1FC91A57D4B7001C107D460C9D6BEFC
SHA-512:	B1BB3371BF5EBB5F63608E6F0A89B552BC5052B006A23DD3C57A4DC8A59B498BAC1F457F21994251946169AB0E3C49FA5F19E8BFCDB3E60CBEA9A7665095632 5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\400835a9-cc7f-49eb-ad83-2afe43e1d9c8.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1645819715.899027,"host":"Cj91Q0e2Rfo4FGbsbrX3sgvvrqjJ1D6z40yaMuxr+W8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283715.899032},{"expiry":1645819724.862239,"host":"CtM6FnbQ8oC9tJB3kpCUAB/2Qfhm+sAvGid3anqO8pc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283724.862243},{"expiry":1625170125.068152,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283725.068156},{"expiry":1645819723.711108,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283723.711112},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1630008459.847033,"host":"ZQKa9hHvZrC6YYMmCzSeRy4pyeERJJ1/HmyHfa2RG94=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48d2f0af-f63b-4d5d-9157-999fd13b265e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22619
Entropy (8bit):	5.536191370484228
Encrypted:	false
SSDEEP:	384:PP7t7Ll3hXZ1kXqKf/pUZNCgVLH2HfDwrU1HGanZ27qJ64p:5LlVZ1kXqKf/pUZNCgVLH2Hf0rUJGanx
MD5:	2FE2733A4760F973660442338B7E41C3
SHA1:	F1287D6FA4C4949743A911DD627DE843E98C3D73
SHA-256:	38AD7991A570A8FE7C351A587019937F0C99F4CA17F5DAE1914C982A1B73B310
SHA-512:	A6522B3DF2235CB63A3EB34B10129C3449544395BCE54B542534C7172BCEABAF47C134E40C23F810FA148C53A25BF63E0CA8D7C5603C0053F0D48EC2A7E79BE5
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13258757256981609","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b1206d3-c967-422d-a0c5-828ac5b9f6fd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1374
Entropy (8bit):	5.574737498171495
Encrypted:	false
SSDEEP:	24:Yl3wUZS6H0UhsSCXUjWG1KUl/zkq/HeUe8zUe17wU0RRUeiQ:Yl3wUw6UUh+UjRKUlgqPeUekUe1wU03t
MD5:	4FBEE5AADDC634F169F53A9C4DE7290A
SHA1:	DDB7109AA0E60D5539AC4A6751FB68A30FC4B303
SHA-256:	294157297B4F5C225EB846431E2125BC98BB2ABF03DA9EA50C820BE1B9CE4083
SHA-512:	571252AD9D1E57B5CFC326779083EC88F95CD8FE8D39341734F7F7840B40CA88BC4C000DA9EAA8328D013E4333233C10ED5EE29BDD210CDFDCDA727E10208A8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1645819661.077842,"host":"CtM6FnbQ8oC9tJB3kpCUAB/2Qfhm+sAvGid3anqO8pc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283661.077847},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1630008459.847033,"host":"ZQKa9hHvZrC6YYMmCzSeRy4pyeERJJ1/HmyHfa2RG94=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283659.847037},{"expiry":1645819660.435199,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DealM38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283660.435203},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6f8ce10c-8687-433c-a333-07456a4f8811.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16763
Entropy (8bit):	5.578521916511229
Encrypted:	false
SSDEEP:	384:PP7tmLl3hXZ1kXqKf/pUZNCgVLH2HfDwrU+79V642:ELlVZ1kXqKf/pUZNCgVLH2Hf0rU4v6x
MD5:	AF284E041A5ADC3C7B780C5E014FE2A8
SHA1:	ADE9816D4BB9E84F3580DCACB0B69108D9F387EE
SHA-256:	B80F09E1DC7D3F2C46DB8AED5E420BEA507755BB5A34053AC5F29901D6BE5C26
SHA-512:	467EF33F2ACEDD935605C4B57035E068567EBD202F68EE6F8FF1AF607B22DAB5D3EAC980528C02B2692D4A4D50893B22AE079091BC7442754F5993F7F5BA77E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6f8ce10c-8687-433c-a333-07456a4f8811.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13258757256981609","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e753abe-b3d2-4451-afdc-42691c9043bb.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3213
Entropy (8bit):	5.596593271825397
Encrypted:	false
SSDEEP:	96:xU6UP6U8UDUkLUbeUOieUoUURjUXpUaUMUL0UacKUaRPeU3UfU03Ug:xU6UCU8UDUkLUbeUaUoUU9U5UaUMUL0y
MD5:	E1A8C992F5B233134C1F561AC3C9AD9C
SHA1:	00EC22C466CE0701D8E6D9ABFBDF53B954E640EA
SHA-256:	4E3212B9F105B887D0CED797EEADA01D8E953C4A51E4F60F24B589E74CCB4393
SHA-512:	1F9CC94F3BE264F399DDE347994F3C759658C7BB311AD11276742BDCC9A50662002D7506B6C512A8634C2CB0C83761A466ADAA2A70A6C3A40BE51F178F11F85
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1645819715.899027,"host":"Cj91Q0e2Rfo4FGbsbrX3sgvvrqjJ1D6z40yaMuxr+W8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283715.899032},{"expiry":1645819732.38938,"host":"CtM6FnbQ8oC9tJB3kpCUAB/2Qfhm+sAvGid3anqO8pc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283732.389385},{"expiry":1645819732.633487,"host":"C6hhjoa/UfPQDtK7OhzQayqV5YYV+Gd1zl/FgGIO4iI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283732.633491},{"expiry":1645819733.612301,"host":"DHQ6XMHmN74TG6qlJx95bT4n+y90NNG3hBMVruRe6EI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283733.612307},{"expiry":1645819726.94387,"host":"GUMBCxLSZCR4SQZwNKF01+nd82RrNQf4e6FIoaTS+0g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283726.943872},{"expiry":1645819733.014773,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8669df51-e298-485c-bb04-c3e9a6943a24.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	3381
Entropy (8bit):	5.594910927486101
Encrypted:	false
SSDEEP:	96:xUFUAUZUMUkLUbeUOieUoUUDjUCnUaUaUL0UacKUaRPeUYUBUfU03Ug:xUFUAUZUMUkLUbeUaUoUUfUCnUaUaUL9
MD5:	BE7874EA2E0E1FAA76CCF80D775085B7
SHA1:	69F02E44CC5AB35352B60462E136A7EC96C5D6F1
SHA-256:	BB7ECD102882958057E729466768B329B13A25502D6D7A218FDD4BB2101CBC2F
SHA-512:	30DDAA6C1F7604D63D1BB3070E402DE920B69E64AE907FE4AE21B51187B3C19EC1ECE26A5BBB05F84D7B0ACEE82A06BD1223F8167829EDF307F6859D05E12E11
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1645819715.899027,"host":"Cj91Q0e2Rfo4FGbsbrX3sgvvrqjJ1D6z40yaMuxr+W8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283715.899032},{"expiry":1645819744.552607,"host":"CtM6FnbQ8oC9tJB3kpCUAB/2Qfhm+sAvGid3anqO8pc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283744.552612},{"expiry":1645819763.141702,"host":"C6hhjoa/UfPQDtK7OhzQayqV5YYV+Gd1zl/FgGIO4iI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283763.141707},{"expiry":1645819745.01514,"host":"DHQ6XMHmN74TG6qlJx95bT4n+y90NNG3hBMVruRe6EI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283745.015216},{"expiry":1645819726.94387,"host":"GUMBCxLSZCR4SQZwNKF01+nd82RrNQf4e6FIoaTS+0g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283726.943872},{"expiry":1645819733.014773,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\95d161ed-4900-4609-8d96-8f77a1b9226c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3213
Entropy (8bit):	5.5983843191842615
Encrypted:	false
SSDEEP:	96:xUFUQUJUMUkLUbeUOieUoUURjUXpUaUaUL0UacKUaRPeU3UfU03Ug:xUFUQUJUMUkLUbeUaUoUU9U5UaUaUL0y
MD5:	7AA6196671F737328E851398F1783738
SHA1:	1ABFEBA88FBED1CA0C8C05E3B13417AF16F7AA6D
SHA-256:	43D844229F5999511C848B9FDD0B535DD66A0AF5B535FD338C3AFD195122405F
SHA-512:	7B60D426B9EA309A3A3E377C2E663460CF91A074AEC73F2F7CD054FD3660C021F0D314F7D4D7ABEF9F1773E65EB1ABAD3482638DF8634E86197DAF2EEF8D7DA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\95d161ed-4900-4609-8d96-8f77a1b9226c.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1645819715.899027,"host":"Cj91Q0e2Rfo4FGbsbrX3sgvvrqjJ1D6z40yaMuxr+W8=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283715.899032},{"expiry":1645819744.552607,"host":"CtM6FnbQ8oC9tJB3kpCUAB/2Qfhm+sAvGid3anqO8pc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283744.552612},{"expiry":1645819732.633487,"host":"C6hhjoa/UfPQDtK7OhzQayqV5YYV+Gd1zl/FgGIO4iI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283732.633491},{"expiry":1645819745.01514,"host":"DHQ6XMHmN74TG6qlJx95bT4n+y90NNG3hBMVruRe6EI=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614283745.015216},{"expiry":1645819726.94387,"host":"GUMBCxLSZCR4SQZwNKF01+nd82RrNQf4e6FIoaTS+0g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614283726.943872},{"expiry":1645819733.014773,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.218586309855661
Encrypted:	false
SSDEEP:	6:mNyw8d4q2Pwkn23iKKdK9RXXTZIFUtpeywCu9JZmwPeywE9DkwOwkn23iKKdK9Rn:ElvYf5Kk7XT2FUtp0b/P0EV5Jf5Kk7XH
MD5:	44B9694BF8B23513A1D9380111148009
SHA1:	5D601F61A999599FF39F08D43928CEE05E0856B3
SHA-256:	0DC530DE61DE839CCD6629123C8E6EB7EDCB45B8FBFDEA4DA9AE4B4AE87F9BF6
SHA-512:	4D7457C1331C657F541BA81EDE7D49BAAB98F7BB8A24C9B854DBD250D551EB66429A310925878F3D0945DAA21B5B18178E3ED35D973E03E3453691DF4848548
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:07:48.606 1b80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/25-21:07:48.607 1b80 Recovering log #3.2021/02/25-21:07:48.608 1b80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.216644133350917
Encrypted:	false
SSDEEP:	6:mNyw1N+q2Pwkn23iKKdKyDZIFUtpeywGSZZmwPeyw+5VkwOwkn23iKKdKyJLJ:En+vYf5Kk02FUtp0N/P06V5Jf5KkWJ
MD5:	B800F1D81F5143276D2D3935B62BBDCA
SHA1:	A8BEDE90BF4D046C7AF9A284825FB25582A06EDC
SHA-256:	05BC8B32038B6A8C5C266DB4995DE720CE90417085B1FB57F92663DB02EA4FB7
SHA-512:	0DD7AA3B4033DFF5C19ADAB0692F1FF7F543C8D150400174519E895486B773A93E3A54A08DFBD7D22D01C65B75CBDBEF057073907630A1184D7D9EFFCB2BE05C
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:07:48.482 1d4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/25-21:07:48.620 1d4c Recovering log #3.2021/02/25-21:07:48.621 1d4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04c791db684b9b0e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.519321919657342
Encrypted:	false
SSDEEP:	6:mhnYGL4SudL/ChktR1IBmuxFudRFgQgQw/EnhK6t:Rnt/Chs3u6Ngo
MD5:	B531DD6A75220E2619A75382A256B6B0
SHA1:	B7592E88E79F5C803DF802770D0B3C39D8DE46E0
SHA-256:	EED5FBE7F4EF22662D3E351019F31B452C8D3389ED87825E1EDD350B15216EF4
SHA-512:	C1E74073682DCC957787DEDBEF268A5890B9E00261070719686B4A0A6C006E3F1439E97B14A757AE2EB8510E07DAA8732BC507B28285A933B5262DEC2EF807D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...CO....._keyhttps://www.miamidade.gov/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js .https://miamidade.gov/U...../.....x7.....yR.....@.....K...sAL.4..T$.E.A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07224a0d300bf0c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07224a0d300bf0c3_0	
Category:	dropped
Size (bytes):	1231
Entropy (8bit):	5.3604285871155435
Encrypted:	false
SSDEEP:	24:w70hKiDZisYyvrJlAGFZsZv2amDleeXVajTewEt:60QasVRm5eeXASLt
MD5:	30D64E57742BC1AAAFADFA8C5AF93976
SHA1:	B80D6BD5C21C64556835ED7C201BF98CC90AAB26
SHA-256:	1AAEEE78E82AE621DDAE67919E632E25CC6275B3C8B871ADCEBF0C41FE864A40
SHA-512:	E0B33BEC96F300FB988E24B5C8A2E23AC949CB15E996780DDB148E02F64506835487AD96627E25D70B64A6BA21F99803B2D7A5E17656016F0E2586014DEA3B84
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....2R`...._keyhttps://www.miamidade.gov/resources/js/md-global.js .https://miamidade.gov/.-^.../.....1.:.....k.....F....c:.A..Eo.....,.....A..Eo..... ....-^.../.....'.x.....O....x.....i.....L.....(S.T..``.....L`.....(L`.....(S.....IaZ.....d.....QcN.t.....resizeIdE.@.-....@P.....3...https://www.miamidad e.gov/resources/js/md-global.js.a.....D`....D`....D`.....\..`*...&...&....D&.(S...Ia.....d.....0.....Qd.....backToTop...E....d.....D&.(S.....Ia.....Qd6..... .doneResizingE.d.....&.(S...Ia.....Qe.5.....pageNavAnimate..E.d.....&.(S...Ia....v....d.uO.....".....#.%....&.)....*.*....*.,....-...../.0....0.2....2.3....4.5....:.:.... ....d.....(.).....d.....+.,.....IE.d.....D`....DI]d.....`.....`.....`.....`.....QcJl.J....document..Qc.c=.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\09aa4b2a50563c7a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1813
Entropy (8bit):	5.383461573039955
Encrypted:	false
SSDEEP:	48:J4NZ6/TirEOrlPUBhD5gcHHw45ahWcOQ4Ut:J9/GxrRUXnIWNQXt
MD5:	6D1F680DE15CB06D9384458E92A24FD5
SHA1:	297510C5DD014E29E6966BBC6A8C8FB8AC141EB3
SHA-256:	81F6E9CBC94DF1DC2AD566A0C1348FFEE9D13CD24C38C885EBE7346CA62AF832
SHA-512:	4DC0834A9802FA96E8DA3AC0FA74BE6F1BBA201B45598AAE49AC6D29A22952B3EDDF8667BB3F7927AAFDB07A13EDA916C28CECF27B61CCDEF422BFBC1A98E5D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,....._keyhttps://www.miamidade.gov/resources/js/1.4.1.jquery.cookie.min.js .https://miamidade.gov/..c.../.....,_S..].;..x..D...G..~....9O...z.A..Eo.....F .....A..Eo.....c.../.....'.....O.....G.....(S.8..`(.....L`.....(S.p.`.....$L`.....Q.@j..'....define....Qb.....amd.....`.....M`.....Qc.V.....jquery.. ..Q.@.&.....exports...Qc.e.....require.....Q.@.;?....jQuery....K`....Dv.....s.....&.(.....&.z..%&.^....'...s.....&...&.]...&.].....&.].....(Rc.....I`....DaX...F.....e.. .....P.....@.-....PP.1.....A...https://www.miamidade.gov/resources/js/1.4.1.jquery.cookie.min.js...a.....D`....D`....D`.....0...`....&...&....&.(S.x.`....8L`.....hRc0..... M....O...Qb.Hf;....c.....Qb.....d.....Qb>y.....e.....QbJ.....f.....Qb..h....h...g$.....I`....DaX...&....(S.....Ia.....q.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fb33271053e6b85_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.602255318466472
Encrypted:	false
SSDEEP:	12:AGB2u5BKFguGzz/FFJ8uYNcFFJkleYEFFJj:jsQKFA//FFJ8XNcFFJklHEFFJj
MD5:	3B5F2558859398EAA03A11DD1F02AAB4
SHA1:	CE148F0277B23A78328D11CC62E31FD34D755D7D
SHA-256:	BD253040B5D322E97E17D52BAB1D8EA3276DCB11EAD27249B8F4072267328FFD
SHA-512:	61EFD74629D13C66A112E6D3B56C62B23F2CB7D97861982CF3BF1F4BDD13E0F386913FBD2B4C895E146DAA3B2911FFE0A3092E3297D0F3847E42B0891EC0180
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...../.....keyhttps://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/base.js .https://youtube.com/..}.../.....J$.....zQ..-..)p..I9%?....MY.d....%X ...A..Eo.....A..Eo.....}.../.....$.....zQ..-..)p..I9%?....MY.d....%X...A..Eo.....}.../.....$.....zQ..-..)p..I9%?....MY.d....%X...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12bf4d173f54450b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50552
Entropy (8bit):	5.912231442210841
Encrypted:	false
SSDEEP:	768:dkSeOEko6BlM6l7i+j6AZdb7jE0CKYq9WBE0CSyVIoHWGYNEW7sTNAyX3FOuntXg:ddemDBr7i+rE9KYqWbCbI/GgVlhXld
MD5:	D584A8A57752C5C487B653CA8AE0163A
SHA1:	781D4F8C2348A5DD52AFA495CB4D248699268D9B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12bf4d173f54450b_0	
SHA-256:	E783C90B874FA2E951ABAFD3D7F1F70EAF8EF5794624D30A74C9FC05C6094217
SHA-512:	DFE5BC740EE3A68D940C5B344CAB176E53A6D372865CA604240FA6BFFEA0CB4C8224A756DF855ACCF919B2A998EC86EE25E0C688D8115B9732F5EC50D9BACD9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....ip....._keyhttps://www.miamidade.gov/resources/js/moment.min.js .https://miamidade.gov/..c.../.....t.I..BGnY..A...e../8.*...}.kM...A..Eo.....A ..Eo.....'.A....O.....6O.....X%.....t.....(S.<..`4....L`.....(S.l.`.....L`.....Q.@.&.....exports...Q.@..i....module. ...Q.@j..'....define....Qb.....amd...Q.@.O1.....moment....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.]....\..&.-...%....(Rc.....l`....Da....(.....e.....`. ..p...@.....@.-....@P.....4...https://www.miamidade.gov/resources/js/moment.min.jsa.....D`....D`....D`.....=....`....&...&....&.(S...Y%.`jJ.....L`R.....q.Rc.....R.....Qb>y.... ..e.....Qb. A.....t.....Qb..s....n.....Qb..e.....s.....S...Qb.q.O....r.....M...Qb~*.,....o.....R....Qb>T.....l.....Qb.....d.....Qb..h....h.....Qb.Hf;....c.....QbJ.....f.....Qbj.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\167b0645db408709_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.92847534072782
Encrypted:	false
SSDEEP:	6:m0YE54MP44u0mudJZgul0/pJZK6tQBuvtGhgkaCbAQuH/pD:V5XrJv1MrTmsvtGCkaCb4
MD5:	6F93F963BEDC359C1294DD5058E991E1
SHA1:	BA92F8CD55F17D0B6346C2E1568CD355B428A3C7
SHA-256:	EA02A8B460E726F13EC7CA55F033530835B66F48A044214EEA63FB5ECB44AB2E
SHA-512:	C8E9604710B1D3D151305F662276420E5DBFC6C9D72825E987AFC4B39EC96D125BAA17D89A685F6CB53F3A2E7B1350EA14DB1757D51441D16B45EF83B61158B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://cdn.levelaccess.net/accessjs/YW1wMTI1NzY/access.js .https://miamidade.gov/..~.../.....+#.....B...._*Go....L....Lq.a.$7...X.A..Eo..... .....A..Eo.....~.../..6..499AF2F6AF3231A7B7182FF68C7BB4FCA557BEA60F20F442154A1F3528A858B0..B...._*Go....L....Lq.a.$7...X.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1696134080d701e5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.437428904119229
Encrypted:	false
SSDEEP:	6:mKPYGL4SuddbZtudTkz/+Hgell2C9V8Pv/uDK6t:zgnKXL9cvG1
MD5:	C3275D87DC1750F87E1850D376BD908E
SHA1:	A6142DE6645A82E047713DC91DDA3B835639C82E
SHA-256:	0B35A5A039A3DDC47C26CF635C7441124402E8FE4B3C1181DCCEFD7C55193E89
SHA-512:	D6DF9143F457AAA0770143DB279406AB30121F79B672E3B129E9A047E6E702B7BED5849D14B61E7448EC9AF36A90E798EE9C9B2B561C4D16EFC20A0FA8D5127A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...+w....._keyhttps://www.miamidade.gov/resources/js/1.8.2.jquery.min.js .https://miamidade.gov/..c.../.....g/.){....(....^...s.u*.....A..Eo.....*.r..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1882dbfa36859db6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.570007231672549
Encrypted:	false
SSDEEP:	6:mSYcCud2M6B/pvmudbWgnXO5mNRZR9ozrtRK6t:RwPB/pzlkeRKzx
MD5:	26467C8C39B7C81780E6BD6D4FE6D72F
SHA1:	971A086FC2A6E4B47D26A4EFC4BDAF5632D1901F
SHA-256:	18D9AF1020793A413A51B35646746C6E3FB2CE25CA506E44D23FB6F44B5F1FB8
SHA-512:	7FA66409A905FC068AC165D654ADDF140C68C0B1F6B8CDB605534B7E5B78214884BA09E7C7E7D7CC56BAEC99D3ACB66F95F5945AC04C495C8D4DBD494869BBE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....W....._keyhttps://accounts.miamidade.gov/myaccount/main.4f2d4e416ce339eda3fd.bundle.js .https://miamidade.gov/.C.../.....e....d.{CF.....(.4..... S.....A..Eo.....`<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a99875434b2d16a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25384
Entropy (8bit):	5.68816620368307
Encrypted:	false
SSDEEP:	384:kZ+bZS1cCnkdhhTSUxkiHAdP9lRCK6FM6KMR2M+ohi64yJZFuNx1sWjs+FCqO08i:glghIx9CY6KG2RoojH7yvgW5kV4zpzAP
MD5:	28CDE73943ACA60B3324DE698622EFBC
SHA1:	C5FB593BA01A49A05DF787EA676ADF72DF2DD9A2
SHA-256:	6D4912D9CA81E54CC2DE3D4559C3C785CE66D1CCCED1A6EE5519CC2B81A76194
SHA-512:	1741FAF75DE7532970B819FA911E51AB5D6D4A51C73BEB5D3EF89FCA62D948A54A973BD80252A656A4AA7FA38270EF3AB732F727F5C654730B271AE7579E607A
Malicious:	false
Reputation:	low
Preview:	0\r..m......h..........._keyhttps://platform.twitter.com/js/timeline.217a220423d55b36c29099c89d1abb2d.js .https://miamidade.gov/x...../.............&.......$'rc.A.'.].&j.5.I,.w?.2l .&....A..Eo......x.{..........A..Eo................................'.[U....O.....a..i.o.........................$...............\....................(S.....`.....xL`8.....Qc.KW.....window....Q.P.E......__twttrll.....Qbz. ......push.....`......L`.......`......Ma........`........b`.......d...C`v...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`.....(S. <.`0.....L`.....0Rc..................Qb.q.O....r...`......Qb........178.`......Pc........push.178a~........(S.8.`*.....L`......Qc2P@.....isType...u...K`....Dh................&.(...&...&.Z........,Rc.......... .....I`......Pd........e.exports...a................b.............@.-....XP.Q.....L...https://platform.twitter.com/js/timeline.217a220423d55b36c29099c89d1abb2d.jsa........D`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aab6f08cdf296e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.940842698690585
Encrypted:	false
SSDEEP:	6:meYsxH4Ao8RA7Vk6xSzSuenTYNR1z7Sud51Jy0fWMV94udWFgMtVRUooot4ZK6t:/H4AvROVkASqUNR1fnn1Jy0fNTAnuloe
MD5:	7F6CBDFDC6FEDE2B9FE785952806CCBB
SHA1:	0995FC9494BAA9D6132D02D06D2C832E1D063FA3
SHA-256:	19937AEBA89A07819414C628E73DCCA84ABD2F13655213A14E041B39E139D90C
SHA-512:	1471248AC1B4FE22CD841D2E80E38FED666F1611F22C37ABC8B72D0A5BA147E0D58623F6F903B3E6AC6F08CDFBC509C0838D23891AA7AB64E32D3D895D7C48 9
Malicious:	false
Reputation:	low
Preview:	0\r..m..........j..u...._keyhttps://zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com/WRSiteInterceptEngine/?Q_ZID=ZN_a8zTa7cUf00EjMF&Q_LOC=https%3A %2F%2Fwww.miamidade.gov%2Fglobal%2Fnavigation%2Fservice-index.page&t=1614283715066 .https://miamidade.gov/.s..../..............p........-....N.;..|..N.;j..i.....D.A..Eo.. ....([p..........A..Eo..................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ac412f89d4b472c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28440
Entropy (8bit):	6.100484090444957
Encrypted:	false
SSDEEP:	384:hYlpWYRgyq+e8qugvRUUwrC7mnEP7wWL4ll+gU4mATsO9byKMkWb:w++1RgvWUGC7mnEP0WLM7vmAAOsVkc
MD5:	387C2B3B66521ED307AF26E7BB2D73D7
SHA1:	6F69384F64034C3A2BCFC965F7D8C9F836DBAE55
SHA-256:	7CC87F0F89556F662743F26D948CC64E7046A615F01590DD84B423A493B9DC4C
SHA-512:	23C743D7AD299BBDE6B6B7DB7E68379D8D1B60C57F2EDA3F1DA42637BE425FF85B927E8D96DDF1100ABFF0AA893C8E55CFF2475EEF3CFA93AC0F88C1A5F13 B94
Malicious:	false
Reputation:	low
Preview:	0\r..m......d......|...._keyhttps://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/embed.js .https://youtube.com/.:..../..............%.......h@.H..K.[[.e..........h.5p@ f....A..Eo.......X..........A..Eo..................:..../.............%.......h@.H..K.[[.e..........h.5p@f....A..Eo......p..(.....................'..u....O.... m...5.................p... (S.4..`$.....L`.....(S.E..`B......L`T......Rc............z..........Qc>......window....Qb.px.....Q2....Qb..v=....R2....Qb..$.....uGa...Qb2!......S2....Qb.Ka.....T2....Qb.\?.....U2....QbJ.C. ....V2....Qb".Q....vGa...Qb........W2....Qb.......wGa...Qbb..R....X2....Qb...J....Y2....Qbf.B]....xGa...Qb.z.8....Z2....Qb.i~.....$2....Qb........zGa...Qb.Ng.....AGa...Qb.Q......BG a...Qb.9.E....CGa...Qb..;.....EGa...Qb".sY....FGa...Qb.......HGa...Qb.Ip.....GGa...Qb...z....JGa...Qb.&......LGa...Qb..xD....MGa...Qb..;a....NGa...Qb.=H.....b3....Qb.=.-....d3....Q b..g....f3....Qb.u......RGa...Qbj

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b04f6e67c0df3da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	261
Entropy (8bit):	5.628992296504076

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b04f6e67c0df3da_0	
Encrypted:	false
SSDEEP:	6:mtnYGL4SuddEIEKQlOInTXLDXcudMFgOcHXG6h+4PJhK6t:UonQlsnbLxS8XZ+2J7
MD5:	B59B4B9F151F2EC1CA6B283A830EBE9E
SHA1:	6E68C51CF6DCAF61D8D4AFBA0489183E0BD90D67
SHA-256:	2FFD8D9C0025A22FBC4F3DC464BE6A4CBD09D704AF1D4EB069C804FBC0B96D38
SHA-512:	E65504CE8F5291F95D5918E879185AFA17FEA2E702C1521EE0EBA8E5CBC361BEB09385A38DD963860DE32B5D88FD17625BFDB5FBE7E253EC6DAA1A46F13A7F4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.N...._keyhttps://www.miamidade.gov/resources/components/search-index/js/runtime-es2015.0811dcefd377500b5b1a.js .https://miamidade.gov/.'..../..... ...@f....."m....."..e9.....F4@..y2.!B*....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\249b940bf2b83f19_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	79104
Entropy (8bit):	5.932151921633342
Encrypted:	false
SSDEEP:	1536:7tVb35mvSxABf59gsQrjyJ5frC2h/GrOFN0LECjbxgVCd:7tVbJJeZ59/QW22h/GreNKBb2Yd
MD5:	B55A32E16087ABF31D9E6F53151FBE05
SHA1:	AADE5D044B3DE5A648634BEA67BAA64F9E655BF1
SHA-256:	C6FAB81C38D44FFDC428A0CD161548082F4D88589389D13379CA26EFDC6169BA
SHA-512:	8D559C370BCFABF099B9AB6A873E5C62369743047F1264B08013C8ECD155D750E981940724B0410ADC1C9D8E5F02DFC38EADAEA145855E28EB1F418DFED02AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...{.....1CE0FD2D9D0A6282D8BA2A9DCD628B237D48ED2E6EF6E4F1222447CFF22862EA.....'..B....O.....3....+.....\#..<.....h..... .....(S....`.....0L`.....(S...]#.`tF.....=.L`.....Rch.....R....Qbv.....X.....Qb.....S.....QbF.-.....G.....Qb...@....za....Qb..s....n.....Qb ...x....oc....Qb.....pc....Qb.....Td....QbZeUo....Mb....Qb..p}....M.....Qb...m....Ud....QbN.[.....ea....Qb.c]s....Ob....Qb..X.....x.....Qb.i7V....Ya....Qb.....na....Qb..(....qc....Qb ..0c....q.....Qb.kbL....y.....Qb... ....H.....Qb2.]....nc....Qb.+m.....E.....Qb.Pq....Q.....Qb~..k....da....Qb..I.....z.....Qb.....Ma....Qb.j.....Xa....Qb.c*.....Za....Qbj.z.....$a....Qb .m.&....sc....Qb*.}.....Nb....Qb.p.....Wd....Qb.k.....ta....Qb.:.....ab....QbV.....bb....Qb..3.....ia....Qb>m.!....ma....QbJ.....cb....Qb.).....tc....Qb.. %....Xd....Qb.<.....db....Q b..#P....uc....Qbj.0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2bc0575a58a7bdad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6829
Entropy (8bit):	5.708135510922538
Encrypted:	false
SSDEEP:	96:jAmCSAcdCA7SYBBPqfqvu7tw465ksY2yb7:0mJAcdP7bPrvKtwpxn07
MD5:	6682ADCFE079E0EBCF2A6AD5911313EB
SHA1:	F9074CDACBA3645B3741A0D82006896C20CECDE7
SHA-256:	9BE15CD6040331E8E5ACB5D019F52DF256A72805B77801CCE2AB5D3103F2A910
SHA-512:	96BFA188643D4015BD7DA1CDAA500737B1089848520644C74C2957FA921F04BB13F33DF772BE74E0C91885817B5E3C0FED8AD20100C6BBFB080BFA1873ABF3C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....c$....._keyhttps://www.miamidade.gov/resources/js/angular-materialize.min.js .https://miamidade.gov/.Ed.../.....4..d*!.Sg...Kz.q.JJG N.....i..A..E o.....&.&.....A..Eo.....'..?....O....(....`.....(S.4..`$.....L`.....(S....`.....m.L`.....@Rc.....Qb>y.....e.....S...Qb. A.....t...b$.....I`... .Da.....(S.....Ia.....(..h.....+.....Q..@.-....PP.1.....A...https://www.miamidade.gov/resources/js/angular-materialize.min.js...a.....D`....D`'...D`..... `....&...&....&.(S...Ia....r.....d..... .f.....(....I...a.d.....D&.....D&.(S....Ia....8.....d..... .....d.....d.....(...I..Q..d..... ...D&.(S...Ia.....d..... .....d.....(...I..d.....D&.(S...IaD.....d..... ....(.g.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c4c7b900e92b883_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.916036866587143
Encrypted:	false
SSDEEP:	6:mLYGLSmXZCLRaFudZWgUOOXuQ+ZK6tB/FTd45jkgjgOXuQ+jK/:IFgznOoHxdKkTO8K/
MD5:	A17D20CDCF69B8BD3F5E8230AAC65875
SHA1:	04486CAFF4909CAD84D674604985F5EE176139E6
SHA-256:	BAC8F35AFE1F6C64D20DA2CF37C9C51F2F839D329B0B2E45D14D31E45F76833E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c4c7b900e92b883_0	
SHA-512:	DFD0DABE79945EE324B746928101B779682EB3E1B0E7FC5D0C29F51348E8DA3D6C588D0553E3FCDA47D3B5E8283390C3CCD6FDFD346FFE3C910D906572607DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...AKE....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-MTLB43 .https://miamidade.gov/>_q.../.....M.....KD.w~...$.....?.9.7.KD-...{.J ..A..Eo .....L.....A..Eo.....>_q.../.....B138BB68B4CE7D9B244853A30CFC1494F09F00A760524D3578663298015DC3BEKD.w~...$.....?.9.7.KD-...{.J ..A..Eo..... .CV..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30a737d3a69dec13_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	352
Entropy (8bit):	5.938525569381186
Encrypted:	false
SSDEEP:	6:m/YsxH4Ao8RA7Vk6xSzSuenTYNR1z7Sud51JyJaECAhMMudqTgcFdv31HlhyAp7H:eH4AvROVkASqUNR1fnn1JyJPt4i2cp
MD5:	882C4E0E52A1A3BF2A0B3133B5B842F6
SHA1:	DB44AADFF425A91BAEC0FEAC365BA6CB7C9F154C
SHA-256:	F26DCC3C3F8EF1F96440D11BA7AA472A1DAAA6329B97493CCECC3FF46CDC116D
SHA-512:	986876EE80BC7C779763C83C06677BF525816F76F1A1167B196FB0F9A1A197C16E19A56BB7387FD7DF8E8D82BBB998D624857DF2F9BAB8ED8F72AFE9FEFD65D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T}...._keyhttps://zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com/WRSiteInterceptEngine/?Q_ZID=ZN_a8zTa7cUf00EjMF&Q_LOC=https%3A%2F%2Fwww.miamidade.gov%2Fglobal%2Fhome.page&t=1614283697133 .https://miamidade.gov/~...../.....}+.....fvD[..pi.:...M...#. :..%. ...+..A..Eo.....A.....A. .Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\335e69ddec2b9ac6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7780
Entropy (8bit):	6.074800084931483
Encrypted:	false
SSDEEP:	96:S9ET+nF7aDynWlYhMf4EPfAtOUJxX5FqKSh0AcTOeC/Wfn7sdcpns4hBGnyJ:sETmF7lIYhVcKSqpTtCOf4dRryJ
MD5:	F77CC2B09FC08B2528C9031F53494D70
SHA1:	54105F9DEDA75604A23BF1B9F3BDF47AED385490
SHA-256:	C149FDBCE46177B1D58E72A0BAFB968789EE3428F54378D196DC16C1AD0F0A52
SHA-512:	4AA48D9E88DC1585007A22DB69C45A4520B460A203113C18E35BB3D26573BB505CFAD2DE4D672A1A5A3B2F430894B52200F086BEFF239FBFD3A85D1C1150AFB0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/BY..../.....&.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....}... .....A..Eo.....BY..../.....&.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....&.....'.....O.....V.v.....(S.<..`2.....L`.....(S....`.....L`j .....RcZ.....$.....Qb>.....m.....Qb&.....n.....Qb.+.....p.....Qb.U.....q.....Qb~.2.....t.....R....Qb..=`....v.....Qb...k....w.....Qb2H.....x.....Qb.....A.....Qb.T_4....z.....Qb>_8..... B.....Qb...w....D.....Qb.0.!....F.....Qb...Z....E.....Qb.....G.....Qb.....J.....Qb...U....h...r.....l`....Da....D!...(S....Ia....#.....@.- ....DP.....6...https://www.gstatic.com/cv/js/sender/v1/cast_sender.js..a.....D`....D`T...D`.....l...`2...&...&....&.(S.....Qb.{.....l...a{.....d.....@.,

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\351a9ecfa9981057_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	735
Entropy (8bit):	5.494657924649792
Encrypted:	false
SSDEEP:	12:X+CGWHvVanTInddN+CGWHvVan2KnZ41N+CGWHvVan7n+:X38idN38x0N38i
MD5:	D87E4463DA5509D18CF754FCA26C5A57
SHA1:	02B1719EBE5D85C7D776A2F53BA6CE5C9B2545D5
SHA-256:	1E2AD9B5F92A8ACC7437B9FA46950F05FBF43ACA8FD8144469813ED12715619F
SHA-512:	9B4EC72A48F46CFB10FE40C2E3E742959A386CF0F9EA34463FAE84E6D8C5B8F41D9F27079BB3DF2368DF61D8C71FC993C25DC661F967E3B6AB980FFE689969D2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\351a9ecfa9981057_0	
Preview:	0\r..m.....q....R....._keyhttps://translate.googleapis.com/translate_a/l?client=te&alpha=true&hl=en&cb=callback .https://miamidade.gov/=..../.....M$.....:/....).....uy.vV....t.A.4.A..Eo.....-.....A..Eo.....0\r..m.....q....R....._keyhttps://translate.googleapis.com/translate_a/l?client=te&alpha=true&hl=en&cb=callback .https://miamidade.gov/.|..../.....?.....:/....).....uy.vV....t.A.4.A..Eo.....A..Eo.....0\r..m.....q....R....._keyhttps://translate.googleapis.com/translate_a/l?client=te&alpha=true&hl=en&cb=callback .https://miamidade.gov/...../.....f.....:/....).....uy.vV....t.A.4.A..Eo.....K.&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\379474f27f093fa4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	76176
Entropy (8bit):	6.068213046827896
Encrypted:	false
SSDEEP:	1536:RmJUCogD8RttIeRaQzNjRbjxgOY/MCDsbViea+EmD6:Rm2CoLRttIrQzNVHxgOK9w5iHBmD6
MD5:	7C3E4162F96D43780733C37608CFE5BD
SHA1:	1D3C14E7B554097E4EF0B24C4A5ABC663F62790A
SHA-256:	D1FD032767689BC5507C29F9EBC49171E11E00FC5F7A6B5C3342FEC8B306560F
SHA-512:	0A68385830CB05A6072E0E98C37191AFFE49C5264D1C1558E735D5ADEF389C1D66E868DB285AB2301F4050A8CB28B14507EE5A463A8E833B66D5347554725F27
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....A97E5F671E87D8B0724C0A53FF602B49B9DFE1065092096EB5995E0357C9B3F1.....'.....O....P(.....h.....$.....|.. .....8.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....QbZ.~....n.....Qb2.....q.....Qb^t.....r.....Qbj..V....t.....Qb.....v.....Qb...c....x.....Qbj... ...y.....Qbf.Z.....z.....Qb.R.....A.....Qb...g....B.....Qb.j.F....C.....Qb..}.....F.....Qb.....E.....Qb&.....D.....Qb..j.....G.....QbN:.-....H.....Qb.....J.....Qb.ssJ....I.....Qb.....K.....Q bz.....aa....Qb6r.I....L.....Qb.Y.....N.....QbB<.....O.....Qb...f....P.....Qb..ef....M.....Qb.`.O....da....Qb."....ea....Qb.....Q.....Qb.p.I....S.....Qbb.T.....R.....Qb.....ia....QbVT.....U .....Qb.f ....ha....QbF.....T.....Qb:.F.....V.....Qb*mOG....W.....Qb..~.....Z.....Qb.V.....Y.....Qb..%.....X.....Qb*fHE....ba....QbZ<M.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3be85e22793a2261_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.31825983093128
Encrypted:	false
SSDEEP:	24:sClmDt2joITxCrjp1Iy9Ev/YZ9XQCHksW9FIfMaQYm1LWi9MtFgte3Al:smmDt2/TArj42FWBXI05YNi9MtGcQ
MD5:	08CFBA79956F80CBE29CF49739EFC626
SHA1:	5BB39529E640E594166E46AB22EA4D55C42B31EC
SHA-256:	7D3BC90EA1912F58F91F0C3A19D89E6C8B0E0ECD15BE0C4D64743B2130F70D53
SHA-512:	C7299745DE5466AC50AAFE5B8744893AA377608FD4DC3B05926D354788C930AA1D46D214F468F7DCABB79781F700DF743FE7E52361D1B2F400CB1DB6ACFFA31
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://www.miamidade.gov/resources/js/flexMenu.min.js .https://miamidade.gov/ZTc.../.....no.....v..n....o.j.|...z.A..Eo.....p.....A. .Eo.....ZTc.../.P.....'.U.....O.....(S.8..`(.....L`.....(S.T.`^.....L`.....Q.@j..'....define....Qb.....amd.....`.....M`.....Qc.V.....jquery....Q.@.;?... .jQuery....K`....Do.....s.....&.(.....&.z..%&.^.....&.]..... (Rc.....I`....DaR.....d.....P.....@.-....DP.....6...https://www.miamidade.gov/resources /js/flexMenu.min.js..a.....D`....D`&...D`.....D...`....&...&....&.(S.p.`.....,L`.....PRc$.....Qb>y.....e.....S...Qb..s....n.....Qb>T.....l.....Qb~*.,....o...d$.....I`....Da..... ...(S.....Ia.....d.....d.....(S.....Ia....F.....q...d.....Qc.KW.....window....Q.@...(....resize...(S...Iaj...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cc37ae85ca32abc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.822437091774266
Encrypted:	false
SSDEEP:	12:aj2E3EUjwux2pHgyyN3CMxhHfnn1Jy0fNZy0CBsU2v71:a6E0UjwuyAyyNSW146NtCSUM71
MD5:	AE8BBEEC9890FE8AACC2BD3AB0E4CDF2
SHA1:	9863F64BCE0C4929A67E84ECFB06AF5D15D7E374
SHA-256:	BFD2B7FAE06E07DA4BF510370DF2A7941EE2006E8A11F81EBC18CC9388EE4F4E
SHA-512:	7774A1779C37B3DC4C65D91088A469800CFB5961F973DBAB52377544FF8A091B3C28E725F0687D38FD200622C26CF56D334CBBABE22DD9A9C853C789D88F603
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/950153867/?random=1614283712003&cv=9&fst=1614283712003&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=60&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg2h0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.miamidade.gov%2Fglobal%2Fnavigation%2Fservice-index.page&tiba=Services%20%26%20Information&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://miamidade.gov/Bj..../.....d.....p...#..].-.'c..{.(xC.S..,P<;..A..Eo.....t..J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cdbf274a556cee2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cdbf274a556cee2_0	
File Type:	data
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.674908180933358
Encrypted:	false
SSDEEP:	6:mmQgEYGLIqlQEVDkxWVLguGRpgJiR7uvbvAStbK6tKgAsR7uvbvAEh:PtqlddguGkiR7qltNosR7qr
MD5:	828B2D5EEF8B213843250C1C0E018984
SHA1:	5995B5FC23FF2C3EA27F0E0122219A361BE3BC3C
SHA-256:	A75F2105C181BDE0A220FD77970E58A4FB028B710DFB5ED4CB345013810DBA6A
SHA-512:	3B5DA22CB7D495C4D52EA506A1697777367240DFA7A35EC9FBEB4EF23EC094F4E03619A5923388FDD9A418026EBE1EEFC25FB4FFB0D99D25A3A4BA961F2BA295
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...yS....._keyhttps://www.google.com/js/bg/5F6tG6N9C-HNFBmbPVEyNyk6q7IXWibXNpfQ51AyKrE.js .https://youtube.com/...../.....%.....`...@.h=...p.8@V4.l.*.Y...]k.;e..A..Eo.....G.....A..Eo...../.....%.....`...@.h=...p.8@V4.l.*.Y...]k.;e..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ee130f137310dbc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	413
Entropy (8bit):	5.686137195569649
Encrypted:	false
SSDEEP:	6:mD9YEDLBHEuXhM66il5VhREPK/MWfSudr57kgzK6dTTxIL/ReuudiXgVFVndwukB:alDLbRuWRaK/3fnZVzK6dPNtFZuCbyR
MD5:	BE1562E99B9A23052B9463980DEBB635
SHA1:	AA998A3F49157C3DE5F8846A643EB048654C09F7
SHA-256:	DEA547668179468CA5FA839091C919242276A216DC2FA0D35C7710A4E201EA69
SHA-512:	455A63D9BE9FD7094BEC90C0E7F231AC80106561330EC7FA8D6137F856D88FFC2E460AE95A01DB75E9B69062E8515E53B06A85ECBE01D267AEEDF0300630088
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h}....._keyhttps://cdn.syndication.twimg.com/timeline/profile?callback=__twttr.callbacks.tl_i0_profile_MiamiDadeCounty_old&dnt=true&domain=www.miamidade.gov&lang=en&screen_name=MiamiDadeCounty&suppress_response_codes=true&t=1793648&tz=GMT%2B0100&with_replies=false .https://miamidade.gov/`X..../.....(.....A .t.....`.....1..C.[.....g...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4049cff441731e44_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.764325523420168
Encrypted:	false
SSDEEP:	6:mT8EYKxDCuudwg0+xi84fkbhZK6tzl8+6skxk4F+IU+xi84fku:ktg7LOWTnNkdVLO/
MD5:	614B6C725FBB9D7D42E9D817332E0C2A
SHA1:	586E30BD48193E51ED1517CCFF59CB3627F28F08
SHA-256:	C2F49BFBEB5B132E47F1A1CD99B92E632BA4DB97F379213AEE0CC0009320F39C
SHA-512:	71AC5E01F3E381576279B5AC0CC58671403D20C082CC4C8C822077188EFCFACF1500A9F2DD3A2E19D1936548AEC380A604E1F16B50D8CE46D8B04E49F22A299
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C.....R....._keyhttps://platform.twitter.com/widgets.js .https://miamidade.gov/.!t.../.....3.....(.....TU...[.ne.CJR-xC..tb..`.p.A..Eo.....lm.....A..Eo.....!t.../.....A880ED45903B7025D4DA8E6A2B8CE28E8DA88B07EAF1A9F0B74B9C485FADD134.(.....TU...[.ne.CJR-xC..tb..`.p.A..Eo.....s)L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\429ebb45cfc87783_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2636
Entropy (8bit):	5.430605996583053
Encrypted:	false
SSDEEP:	48:f4r8CqgwZXWn1UeOG3Rxv3SUaXcWLpngvQbQvf5QS/7I/J/EyTJf/:gm76PvRaXpdKWQvf5/TIVX
MD5:	66DFBD44F36B3A2104042259F3760E71
SHA1:	653C8E478A8285F557F9463AFB9CA127A2467418
SHA-256:	1BC1527EF2F8FF514DD9EBC4F4B995B8E9F8F27769563D2FC38E7CE53CA3F204
SHA-512:	4D0664645F207363704A9C88D60FA0137905B9A1FEA1B6CE13DABC9D726A089DCEC1E001D6CC93D03F43B7B27A4BFFA2ECC45615AA3863508DA5B0CA1763775

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\429ebb45cfc87783_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...m0Z....._keyhttps://www.miamidade.gov/resources/js/global-scripts.js .https://miamidade.gov/..c.../.....R.q.{c../.*.M/x{%...\{.UMU p...A..Eo.....A..Eo.....c.../.0.....'..g....O.....9.5.....\.....(S...`.....8L`.....\L`*....(S.....Ia.....Qer.K.....checkFlexMenu...E.@.-....DP.....8...https://www.miamidade.gov/resources/js/global-scripts.jsa.....D`....D` ...D`.....9....`....&...&..1.&.(S.....Ia.....d.....QcN.t.....resizeIdE....d.....D&.(S...Ia....1.....e.....Qd6.....doneResizingE.d.....D&.(S...IaK...l.....d..... .....QeF.a....checkDropdown...E.d.....D&.(S...Ia.....d.....0.....Qd.....backToTop...E.d.....D&.(S...Ia.....Qe..1.....sticky_relocate.E.d.....&.(S...IaV.....Qe.5.....pageNavAnimate..E.d.....&.(S..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\45324813144077fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	723
Entropy (8bit):	5.469027267073286
Encrypted:	false
SSDEEP:	12:XIe/ZA/XDMeNZIe/ZA/XY7uesZIe/ZA/XJn2ebT:DZ8NNhZ8cshZ8dfbT
MD5:	A5A4AA260760492EC8FE6909F717FEDB
SHA1:	CDF7F3F04E05C9E7CA90164D4EDA40E54DE8CE52
SHA-256:	70078BED82755522BD3C17F10EB8837B622627AD83CBBF612A8CD5B05743DCE8
SHA-512:	9CB274977F279BE278EED00EEF6F49B33D9EC2C3A63ED7625831667073D77EB362F0CA0C6BD9FFBFC2FB7AC222E4296C1E802AF1EB33CEDC8DC5B097768F3B3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...bF5....._keyhttps://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit .https://miamidade.gov/.rr.../.....S.....jD1%.....(.....q..C2.OE....q.A..Eo.....V.....A..Eo.....0\r..m.....m...bF5....._keyhttps://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit .https://miamidade.gov/...../.....>.....jD1%.....(.....q..C2.OE....q.A..Eo.....c.....A..Eo.....0\r..m.....m...bF5....._keyhttps://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit .https://miamidade.gov/i2..../..... f.....jD1%.....(.....q..C2.OE....q.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\49ba72fa34b11a97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97480
Entropy (8bit):	6.1266238620787545
Encrypted:	false
SSDEEP:	1536:AWiIp6ZO1PNofse1+ZkGl52Di1WY//zbUp9HGQOLSwb54OMyWfgZ9T:ASp6Z42NzGS2sY//zbUpJhwSsMy3
MD5:	2BFB35C055713CE62496EE93413E3042
SHA1:	6E1C62FD8D14694C2036CBB4C257B86172D2D433
SHA-256:	A70736E04D679185E6D9AB9404171DB33AD9A2208077FBF2D1D7ED1C82F4F405
SHA-512:	CBF22A8EC9436295B92C119FC02443656345AB642E4D3D3EF8D9F06161706649F7557283C0C831AF0DEB3AFE41CC450F8A87836511451A1C24B0A4458E46C49C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....{....0DE5FC08B902E1A964BE3615257AB1D56641217C902593AF4961EC363218F7BF.....'.....O"...p{..7O.....&..T.....<...@.....<.....(S....`.....0L`.....(S....&.`LM.....U.L`&.....RcP..... .....Qc.KW.....window....Qc.Vtl....minErr... QfB3.>....REGEX_STRING_REGEXP..$Qg&fZ.....VALIDITY_STATE_PROPERTY...Qe..V1....hasOwnProperty....Qdf`N.....lowercase.....Qd~.x.....uppercase.....Qb>.."....msie..Qc.....jqLite...Q.@.;?....jQuery....Qcf.....slice.....Qc...f....splice.....Qc.g.....ngMinErr..Q.@...n....angular...Qe..H.....angularModule.....Qbj0.....uid...Qd.....isArrayLike...Qc.EY.....forEach...Qez.10....forEachSorted.....Qe...`....reverseParams.....Qc..6.....nextUid...Qd62.4....setHashKey....Qd..H.....baseExtend....Qc.....extend....Qc.j`.....merge.....Qc.....toInt.....Qc&tTY....inherit...Qb.....noop..Qc:.....identity..Qc.|n.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ef1b04a94f9eaab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5946
Entropy (8bit):	6.0895331448563965
Encrypted:	false
SSDEEP:	96:EyVQjWLtBqkt0Mx6c/W5od3dyghu2GiMUey4M/evut/YtkefYVQ2fraYaZ:fQjgtBlt0Mx6c/AC/hu71U3eY/Ak7raz
MD5:	2FBBF12F12DCE4A394A7F994AB0CB8BA
SHA1:	BF791008CFF7EAD1D96F37B4EA55405E30EB6CDA
SHA-256:	EAB1CBA22C7F4DF63F321C406D53EECF93A79393713B23C2CCEDC5C4FA02E9E5
SHA-512:	6A0D520C8FC1283F83AE269DE8287020A533345202303185BA8ED91A35C6BC38D3BAFA68F61A09EFEBC494C7FACCDDC1BD069A6B86D6A266DB995B2A8F3BB727
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ef1b04a94f9eaab_0	
Preview:	0\r..m.....Z.....p...._keyhttps://www.miamidade.gov/resources/js/angular-sanitize.min.js .https://miamidade.gov/..c.../.....,_....:..1...K8T..jr.5v....1..A..Eo.....;Y[.. .....A..Eo.....'.....O.....&j$.....(S.@..`<.....L`.....(S....`.....L`R.....Rcx.....4.....Qb..h....h.....Qb.+m.....E.....Qb2E#.....F.....Qb..0c.... q.....Qb^.....B.....Qb.q.O....r.....Qb>..V....L.....Qb..I.....z.....Qb.kbL....y.....QbF.-.....G.....Qb.....K.....Qb.<.....J.....Qb... ....H.....Qb..X.....x.....Qb.....I.....Qb..p}....M.....QbZ. .....N.....Qb..6.....v.....R....Qb..e.....s.....Qb. A.....t.....Qb.O.....w.....Qb.3h0....C.....Qb.YvC....D.....Qbb.....O.....Qbf.9.....A..y..... .....I`....Da.....(S.....Ia.....@.-....LP.!.....>...https://www.miamidade.gov/resources/js/angular-sanitize.min.js..a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\510f12c38eaabfa6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	5.526528486051278
Encrypted:	false
SSDEEP:	6:mOYGL4SuddElEYzXpCmudEgzWW1Bofu40hK6t:wnQInXpC7wW1qfM7
MD5:	205708F718B986EAF98643F0CDFF7DA9
SHA1:	B7959711309489O6CB0D841E15EF9C8F8B40F394
SHA-256:	344F9D8A7889D710A72EABE6F6F20181DDAB9F806ED9C873C047EC8EC8CA5623
SHA-512:	830CADE08468D6C772EBA9131EAF2F925050EB0683ED9EDC610B77553F3F6AA9B466FE558CA38510B9FA0892A4AB5F4C5C8C11785D3C910D26E5E41D7319C2A 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~....z.i...._keyhttps://www.miamidade.gov/resources/components/search-index/js/main-es2015.a417ee09c81b9425955e.js .https://miamidade.gov/]{..../..... in.....b...Ha....24.osX..K1.....A..Eo.....K..A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51828aa6d63df8ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2811
Entropy (8bit):	5.8658553387293715
Encrypted:	false
SSDEEP:	48:BH2aDk+ogCziYVge5IufYWLkxgyai8bOB1OJXhV0JBDdtxoT4s:BJDXxCHge2u+g06JXhVqDdty4s
MD5:	95A27BC644FF1B9AFA4DC6954E84F446
SHA1:	DC31E6DD3240D0FA34A7EF584C4552A7C896EC14
SHA-256:	19482056B7BC01C3A6E0BDDCF68D3E9FF44E8D0603FDAF6E34B701DF9EE6F226
SHA-512:	0FDEC7A57F20B53676EEC3E8E7E0716F3D0D07B1A51A1CF098B71AD6E47CB9428DA6D09C39BFDED7F6E04162CEB1ABCB0CEDF669B57CB63CFF0C411EBAE9 159E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....rJ...._keyhttps://www.miamidade.gov/resources/js/dirPagination.js .https://miamidade.gov/uLc.../.....:.1.....iq]:V ...J.....u....A..Eo.....x..... A..Eo.....uLc.../.....'._....O.....c.f.....(S.0..`.....L`.....(S.1..`.....xL`8....8Rc.....Qd.Us9....DEFAULT_ID...E.a.....I`....Da.....(S.....Ia #...s!...H..m.....$....'.*....-.1....2.4....6.:....<.B....**.....d.....$.....,.i ..... .!...!."".....d.....3.4.....d.....6.7..... Qf...D....dirPaginateDirective.....@.-....D P.....7...https://www.miamidade.gov/resources/js/dirPagination.js.a.....D`....D`....D`.....`p...&...&....&....D&.(S.....Ia##...#... Qf6d.w....noCompileDirective.....d..... .....&.(S...Ia.#...'...4Qk.Q.<&...dirPaginationControlsTemplateInstaller....d..../.....&.(S.....Ia.'...L...4..j$.....Q.Q....T.....*

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58f3e4ae2e487b2e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	20743
Entropy (8bit):	5.751165541849208
Encrypted:	false
SSDEEP:	384:sl+H+aDirtw0E+ocJaTEZRvKf6GH/t5RnOOXfT:kLaD4t4cGCBMPffROs
MD5:	10C54458F5E9C2822235FAF1F9A04652
SHA1:	447D9308DCEBF48852819EE732F85F35AD5D206E
SHA-256:	8E948C5F43BE9FE8BD675D888A0859C95CDC669F3873D16F130D54FF538D1EE9
SHA-512:	A41DE8446A4C4EFCD0F12AD2F74917F1F38B3829C30E4D8302F2326D5D423367ADFB00EE97C783FA237EB9A0FE259D5BCD8A10EC22627B53411EA0F0E78C1F5 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...>..K...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://miamidade.gov/o.z.../.....!.....<...2j...mV...G7....V.X.6.A..Eo.....& a.....A..Eo.....'.O|....O....xO..c.....@.....(S.<..`2....L`.....(S....`.....L`r.....Rc~.....6.....QbV@j?....aa....Qb>T.....I.....Qb.. .....ca....Qb~..k....da....Qbjm.....p.....Qb..6.....v.....Qb.O.....w.....QbN.[.....ea....Qb.Df6....fa....Qb^.....B.....Qb*.....ha....Qb..3.....ia....Qb.0o.....ja....Qb./.!....ka....QbNi.....pa. ...Qb2E#.....F.....Qb... ....H.....Qb.....I.....QbZ..o....sa....Qb.k.....ta....Qb..E....ua....Qb...n....va....Qbv8.....wa.....Qb..l.....xa....Qb./g.....ya....Qb.<.....J.....Qb...@....za....Qb..... ...Aa....Qb..3....Ba....Qb.....K.....Qb.....Ca....Qb.FX.....Da....Qbf!.....Fa....QbRE.....Ga....Qb..>.....Ea....QbJ..0....Ha....Qb^.....Ja....Qb.o.....Ka....QbZM4.....La....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b637dfbcd038651_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.631025810919137
Encrypted:	false
SSDEEP:	12:wgGB2uosPjcRsGguGBWdus+kVFClgs+kXtI1CIs+k:KsqP7GABWgIVFCuIXlCII
MD5:	99AD5424C222BB6A0CA2EFE506C2D333
SHA1:	11CD94C18A7E578E0D1AE1DFEFA6E0AD335C8C82
SHA-256:	A0C0DB528DF09B46255D2EFB2F45A916967CD31BEFB6FBA892C353BA3CABC847
SHA-512:	A6874C6B23FF67D72C41C28EBE1D3E13CFE607DCB136D9288D577B2F535FEDC832DA37FB41B066CBB417CF767A623FF8256892344CCE90A7D421E357C111D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...H.l[...._keyhttps://www.youtube.com/s/player/392133a3/www-embed-player.vflset/www-embed-player.js .https://youtube.com/f.}.../..... #.....Qh.=...)...u..P...>.....9M..A..Eo.....x.].....A..Eo.....f.}.../.....7#.....Qh.=...)...u..P...>.....9M..A..Eo.....@.+.....f.}.../.....y#.....Qh.=...)...u..P...>.....9M..A..Eo.....g.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\641c3cccf0e1412f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.867994723938133
Encrypted:	false
SSDEEP:	6:me8/VYGL4SuddIudX2gQEt/kuq0P4cK6taz/OQCVOJUias0sg/kuq0P4+:UCntAEt/Bq0PVc/CVOo/Bq0PD
MD5:	7F87F8D410A14898B6773F5EEE6FA00E
SHA1:	37E24C76D45200BB44648392438EFABAE8054975
SHA-256:	BFF4354CF61B164B95F43A06C5317F5400F481A567ADDCDF58360118908BD6A4
SHA-512:	9BD91EC57BA10597E15A5F4D58260CD94975369BC5BD4821DAB23D5C23D4AEC441FD6D912F875CA253004F4B714B94B0A506891798721B8BFBAE5C96F625E20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M...u.%....._keyhttps://www.miamidade.gov/resources/js/angular.js .https://miamidade.gov/.nc.../.....)%...z=4F..k.....rO...6qv7...A..Eo.....{.....A..Eo.....nc.../. |..0DE5FC08B902E1A964BE3615257AB1D56641217C902593AF4961EC363218F7BF)%...z=4F..k.....rO...6qv7...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c4b0316c37cc61f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5200
Entropy (8bit):	5.917551507925771
Encrypted:	false
SSDEEP:	96:9jvJNS4vyCbR442PjxWyygsjhqy0uUaokITkjcSb7smKxE1BW26H/i:NfhvjbSbxWVgsj8y0uUaotTkjLb7qxEj
MD5:	6C8B3838BCC41C784C50674AC84FD2E7
SHA1:	E576FCD8121B23C30E5ECD571AE235335E3EEC81
SHA-256:	1063B7A92E95A465955BEA9AE20B062D90F468D9F333091F4599D5691ECBC49F
SHA-512:	BFDB5CDDE3AD14C311D62B69039B9D718DA683A20758B83654B41A8F6844A1D20E88A8BF275A998E56E0F94324B76CAA635D41D8D477F4CACC7CCE90B82129F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...#....._keyhttps://www.miamidade.gov/resources/js/angular-moment.min.js .https://miamidade.gov/..c.../.....h.Z....|..<*..0....4.6.a.bh7`\l.A..Eo.....ql.....A..Eo.....'.2.....O.....(S.0..`.....L`.....(S...`.....HL` ....8Rc.....M....O.a.....I`....Da,....+...(S.....Ia0...\.....1..@.-....HP.....<...https://www.miamidade.gov/resources/js/angular-moment.min.jsa.....D`....D`$...D`.....`n...&...&....&....&.(S...Iaf.....d.....@.....&.(S.....`.....L`.....4Rc.....Qb.Hf;....c...`$.....!`....Da.....)....1...Qc.e.....require.....tQ{....f...Moment cannot be found by angular-moment! Please reference to: https://github.com/urish/angular-moment....Q.@..i.....module....Qe6.....angularMoment.....Qc.....constant. Qf.i.i....angularMomentConfig..,..a.....Qd~,.....preprocess..F..Qcn.l'....timezoneF...F..Qe..nz....statefulFilte

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\745493bd88fa4cd1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	283
Entropy (8bit):	5.82092005888103
Encrypted:	false
SSDEEP:	6:m2YGLSmXZCLRz/7NUT+Lud8KtgcLVWk49byK6t:Xc7NUThH4bE
MD5:	3CE232AE3F3E4D899C54B429E2B23C7D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\745493bd88fa4cd1_0	
SHA1:	C19EA8E86CA53041B4794569B022006852C63F37
SHA-256:	06FC9684FA7438846A66E0E035AE74DC5FAA9DC00BFAFC8C435BC897895F7C0F
SHA-512:	430E4F580E7D7BB7C10D045E0039A0D7D5CA39E8B587C4E51AFEDB66C9D7BDB54B471E15EAADB8EA350AD805DC2540333B9DF5D12C0D2E02BF6209587258A F5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-MN3QTL3&gtm_auth=DXKkIs9VrM65CozSgrWmzA&gtm_preview=env-12&gtm_cookies_win=x .https://miamidade.gov/C.F.../.....|.....M.<.u..r...inL..]%.'.....L....A..Eo.....MS.).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75b95c050691983b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3772
Entropy (8bit):	5.299116027742518
Encrypted:	false
SSDEEP:	48:EKllZ0niyiyGWtJxa35czmlndFxw8J5xC51y7TwYfUdx/fRd5juau+mVySHHACFK:VKiyhtbaLln3xNI3ETFfUHXNP6gCc
MD5:	52C321DB90C67A734D087FF4AD1C8FBD
SHA1:	38BA52853510BFF71D965EE7ACEBD75A7218856D
SHA-256:	304008E6BE328547B5879BAD40F99653FD2A03323CD693185B0470F16BB412D9
SHA-512:	3F2FC3047EFCAD17CEFBC982607EA50C4DF8AD6A28FB9BF0E93BC6E509EF917C34D5CA77D6CB42182FF8E439BCBD7AAEF42ECF4E13CCD8F16AE819C5C8C4 C785
Malicious:	false
Reputation:	low
Preview:	Zo.../.x.....'.f"....O....0.....q&.....p.....(S.=...`2.....L`n.....L`.....Qcf=D...._etmc.....Qd.{....._etmc_temp....q.....Qc&l.....isArray..(S.....5.a.....Pc .....isArrayaj.....IE.@.-....@P.....3...https://110005224.collect.igodigital.com/collect.js.a.....D`....D`F...D`.....p...`4...&...&..q.&.(S.P..`Z.....L`.....M...Qc..2.....callFunc. .K`....Dn(.....(...&..&.%.i....(...&.%.*..&.Y....%.L.&.....,Rd.....Qc.%.....setup...`.....Pd....._etmc.setup.a.....c.....d.....&.(S.....Pd. ....._etmc.push..a.....Qbz.....pushE.d.....&.(S.....5.a.....q...Pd.....callFunc...a....L.....E.d.....&.(S.....a.....Pd.....setOrgId...ac.....Qc. .....setOrgIdE.d.....&.(S.....a.....Pd.....setUserInfoa.....Qd.....setUserInfo.E.d.....&.(S.....a.....a.....Qe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\79eba1d21497755e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	579
Entropy (8bit):	5.818581811188611
Encrypted:	false
SSDEEP:	12:IE3EUvYg8ux2pHgyyN3CMxhHfnn1JyMhXhACBWAZbM:IE0UvYg8uyAyyNSW14MhXhACIA+
MD5:	2A3B9FF5C2F8998F799D820E9D8D4ED0
SHA1:	63C8FDFA32F0E5014D7036AC4EF79D9C5AB3EFFB
SHA-256:	C8A873A51679D49E57CCDA283AA15B36D1EB60B5500CB93B6DAF2B9E8FFE4A88
SHA-512:	14E57895FDC613B6BE0836D652169F9CDDA4ECB7503A7E4489DD4EAEABE1345AC8C9686459CF3178C3D5F9A6AA820DE67DB6136E27008DD22524E9F9A597A9 8
Malicious:	false
Reputation:	low
Preview:	0\r..m....._..S...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/950153867/?random=1614283700614&cv=9&fst=1614283700614&nu m=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=60&u_java=false&u_nplug=1&u_nmime=2&gt m=2wg2h0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.miamidade.gov%2Fglobal%2F311.page&tiba=Contact%20Miami-Dade%20County&hn=www.goog leadservices.com&async=1&rfmt=3&fmt=4 .https://miamidade.gov/...../.....?.....R .b...-....]..i=.....A..Eo.....A..$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\97ed574e9897d66d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.84882217483215
Encrypted:	false
SSDEEP:	6:mhXY8uCXHXOCFRGQAlIXudUgZmD1JJkTyAYMr9yAgZK6t0RZjAOFPnvTDZk2xkTr:xG3VfPIRo1JWyAY3WPj/Pn3ZruyAY
MD5:	D2706A1276D216D799AA3C2998C52C4F
SHA1:	3C0E28E1370EC86C588C3CBD55C236CE917DA7BF
SHA-256:	A28C8CCF33C26EA9FF46DA2166CB2B4B36E98847D4AB97E126E659398E86F26C
SHA-512:	814620252CE1C6D516076051E41B40B90EB10A4382B2C7A7EE1EF413F016E81E04834A3B7F5C0E7149CCE81D593B8E1CEFAED0C67449BD02ABAC2082D4ED48 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\97ed574e9897d66d_0	
Preview:	0\r..m.....p.....'...._keyhttps://translate.googleapis.com/element/TE_20201130_00/e/js/element/element_main.js .https://miamidade.gov/.I..../.....#.....i.._7A...M.U.a....0C.6.3.A..Eo.....[.m.....A..Eo.....I..../.H...5DCA9A9827760BF4C12998DFB67968A50152CD05A14C491AD75D98B2AFE9C635....i.._7A...M.U.a....0C.6.3.A..Eo.....qL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9fecb852ea738613_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95408
Entropy (8bit):	5.6859669279413225
Encrypted:	false
SSDEEP:	1536:QNS92tkxdXJyIQD4kvOb40uKJlbgfNT6Xsefyg4cvSB:Qft+X1Vk4PXgf4vHzSB
MD5:	AC825678AF085381B22D375B6CA01AF7
SHA1:	64CC7EFF095B6CE62726D80C874B81365977F6A3
SHA-256:	6401C921E3E1150F4FE446E03E9EE4570C3580DD17650958A1942DA52FF1551A
SHA-512:	F82840B8B41135B785B73789500BA18FF394BEC5662BB02CB3CCC6EAA27F301F74B3F09FA7A58921BDB7C97588F2651E2D0074B6B9734EE49D5EAA2148A9EDDB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....~....A90D5B3821D677C6CAFBE9246C046E80A587BB0E90DE45D6AE64B7ADC0F5E015.....'.q{....O....`s..uD.....:.....h.....(S.4..`$.....L`.....(S....:.`ru.....L`.....%.Rc.....~.....Qc>.....window....Qb..~.....NHa...Qb>.C.....v4....Qbj. n....w4....Qb.v.....x4....Qb...O....OHa...Qb.K.]....PHa...Qbj=7-....QHa...Qb.b.s....RHa...Qb..y....y4....QbJ.X.....SHa...Qb.."....z4....Qb.X.....THa...Qb.f5.....UHa...Qb.n.1....VHa...Qb^.....WHa...Qb..:.....A4....Qb...z....B4....QbZ..V....XHa...Qb.$.....YHa...Qb.x6....C4....Qb.k.....D4....Qb.. .....$Ha...Qb..1.....aIa...QbR.[.....bIa...Qb.{<.....E4....Qbj.-.....F4....Qb.,x.....G4....Qb...6....cIa...QbZ..[....H4....Qbr4.r....I4....Qb.....dIa...Qb.S.....J4....Qb.Gm.....eIa...Qb~.....fIa...QbV.....L4....QbBd.....M4....Qb.T*.....gIa...Qb.(]....hIa...Qb.....iIa...Qb&.....jIa...Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a11aead48addff6a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	407
Entropy (8bit):	5.553227483559214
Encrypted:	false
SSDEEP:	12:p6bGB2uLgf06guGTpilNuAQz7DPiElNuAQtlilNuAQ:pzsJc6AdmMDPNGIm
MD5:	E8D295F679E10FD512DF54C07A08A6DF
SHA1:	31D806DD361DD105F1827D79E9255C35E7079101
SHA-256:	50F5707E74B7E04F85753C857EFDC50FEB44AD7DA7FDDC2210C1933E044D01D7
SHA-512:	866021191C91B55ED624CE9A6BB04FA03CF655EB82E6D7197C7D93359AD40BDF7EE12D2185115B2BA56EFB7373D9FB418D8E1911C4A117A7ACD7DB7107A07B4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://www.youtube.com/s/player/392133a3/fetch-polyfill.vflset/fetch-polyfill.js .https://youtube.com/..}.../.....R$.....d6V.p..oe.x_.KZ.o.0e(k.....A..Eo.....?.....A..Eo.....}.../.....$.....d6V.p..oe.x_.KZ.o.0e(k.....A..Eo.....c..H.....}.../.....$.....d6V.p..oe.x_.KZ.o.0e(k.....A..Eo.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a97a76e114b8de08_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	5.78425511206382
Encrypted:	false
SSDEEP:	12:aRgE3EUkBTLQOPux2pHgyyN3CMxhHfnn1JyJPlACBXbfvO:aRgE0UkBTLfPuyAyyNSW141lACdS
MD5:	EDCFE3F4274B0511FAA18EFEC1F294A3
SHA1:	5D91E2DAF32CFFE45A99DAB1225ABD8DF9822B64
SHA-256:	5BDAE51B54A7658634B0221A55B4BC385C2CA0F39D83DF18AF897EF4B9D9D773
SHA-512:	3230988F5CAF25E7390EACFBD44966266450442F9901F45EA21F04D74FAA59700A0F76A7100884D554E6BA36C6A8C945DD63C37D0397F7CDDDB59F0AFD66A2B
Malicious:	false
Reputation:	low
Preview:	0\r..m...../.....keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/950153867/?random=1614283694935&cv=9&fst=1614283694935&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=60&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg2h0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.miamidade.gov%2Fglobal%2Fhome.page&tiba=Miami-Dade%20County&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://miamidade.gov/i...../.....%$.....S...6i..}....w.....=d1s;=.A..Eo.....5P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab8ec5c30fbc600e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab8ec5c30fbc600e_0	
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.7359886474039925
Encrypted:	false
SSDEEP:	6:mm8qEYGLIuNvVWJ1hFB7nG7NpguGVKFgWhClqfXwLt5w9hAfK6t:84uNvwJ1hnnGHguGVUCEfX+t5w9hu
MD5:	1C48F456882F08B57A4E75A1C39EFEFF
SHA1:	834F0A07DD305A60ABBE79EDBF958A4C7EEB6EF0
SHA-256:	49395F1BD8B3B1F4AC6584CA154A98EF96B3DD66F49854A499D64F04F4D9E06E
SHA-512:	DB21E8463940D43876E08BF81028C6D54E807B3316203B31B2AE05A60BB035EB4B21AEF86FF0B8A4A51378D8A2CFF740D33D89442741665EF7053E2728E8D781
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....._keyhttps://www.google.com/js/bg/E2xFMTZevhb2jryakLn9w0BayR4vDI5XdlPI-3Ockmc.js .https://youtube.com/.v..../.....(.....A7.r`W}.....e(.rT....U...t.X...A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aff0ca205d48d930_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3434
Entropy (8bit):	5.7626832773719485
Encrypted:	false
SSDEEP:	48:tkL3/TjEReEd4uB/ALwIGZlwIRVlisXLL/+zmWIXYsz1tKvURWAfltQCXpyxL15j:tC/crq4LxTjsURCQCXpU5XDHzsyZCg
MD5:	E52BF039174D29F73FE6F18E59D37C2E
SHA1:	C8FEEF4CC5A5902E3DC1349695A454D4E13F03F0
SHA-256:	29368940178E51321DF0D76C2C7DBFA98A5901E65075FD791819AE1310522423
SHA-512:	77E9E87BEF35AF056DEB23CD6CA2620C42677A3CA190CC29E624D11AE0DBE242A0D7A9C400A9BE0A7B4730EDB505360D04392F7982742C4DBB5C9272209B53E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....d...._keyhttps://www.miamidade.gov/resources/js/purl.js .https://miamidade.gov/9.d.../.....P.^.O..W.k.L..#'.....KLn).A..Eo.....rC.....A..Eo.....9.d.../.X.....'..#....O.....F.....P.....(S.8..`&....L`.....(S.P.`V.....L`.....Q.@j..'....define....Qb.....amd...Qc.KW.....window....Qb.....purl..K`....Dn.....s.....&.(.....&.].....&.\..-.....(Rc.....I`....Da.....d.....P...@.....@.-....<P.....https://www.miamidade.gov/resources/js/purl.js..a.....D`....D`0...D`.....d...`....&...&....&.(S..`P....lL`2.....RcT....."....Qcz.6....tag2attr..Qb.m1.....key...QcZ".....aliases...Qc.....parser....Qc".V.....isint.....Qc..4)....parseUri..Qd>wt....getAttrName...Qc.[.c....promote...Qc..d&....parse.....Qc.j`.....merge.....Qdf.Q-....parseString..M...Qe...R....lastBraceInKey....Qc.....reduce....Qc&l.....isArray..E.....p..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1d1912f2c5eb017_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.4290267783521795
Encrypted:	false
SSDEEP:	3:m+lJq6/lla8RzYP2FycyGrRAJQuFvDvFXJe+A+1/l/lHC1/l7HP1eyzyoKL4hygM:mutlXYe7l0FX5g9NzGoglgrvwhZK6t
MD5:	9AD8B97330649EC446DBB9A16F3757A2
SHA1:	D6E4BA75105FB57B08F9C4D68B9162F31503435E
SHA-256:	14BB9870756F4B85ADFA7704AF1D1ABA863C0C5572D72A53C359381631E8BAE2
SHA-512:	18BDFACDB16DB77ABF94E63B25F255AF1CF7FCE9D3342EB04FE19E88D634DAFE9221A1CEF0A871CF3FD3FB5E16C911EDDEE95512E038029930F5FF62CB6F85A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F.....D...._keyhttps://code.jquery.com/jquery-latest.min.js .https://archive.org/...../.....^;e.....A.+...|..!...o...2.I..A..Eo...../.W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b236d738ed517a04_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	100504
Entropy (8bit):	5.776307902376294
Encrypted:	false
SSDEEP:	1536:bxPMTfTuSNfdFPQPXZu2PpJJvtWPPsqsCirb4eF8dBotiJ9oJ1vAZ1OZo:bx0JDIvZFhfsP0mCRFPtrJ1Kj
MD5:	0EE810688B41ACF90AF64584D5105362
SHA1:	9A8D58C639F464438632DD2FAD4148EECFAEDDA1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b236d738ed517a04_0	
SHA-256:	93FE08726AB45D93B17C86F052DFE24B15F7DDC6B5F991050C2EF0F6DC2B549C
SHA-512:	DED0DBCBC1A764C2107A4D2018259AE27AAAA695E12A993C404FB86E9C46B44AD4D893691BBA4685395A676B7A91048192DFB4E8F693430C6D6385B6C1A9E4B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....B138BB68B4CE7D9B244853A30CFC1494F09F00A760524D3578663298015DC3BE.....'.S.....O$...8.....d..... .....(S.D..`@.....L`.....(S.h.`.....L`.....TRc&.....Qb.O.....w.....e....d.....l`....Daz.....(S.....5.a..... .....a.....Pd.....<computed>.ea`..t...l.....@.-....DP.....5...https://www.googletagmanager.com/gtm.js?id=GTM-MTLB43...a.....D`....D`>...D`.....`....&...&....&..1.&. (S.....`.8.....L`.....Rc.....t.....Qb>OmK....data..QbFU.....ba....Qb~..k....da....Qb.,.....oa....Qb.nx.....qa....Qb.k.....ta....Qb..E....ua....QbZ..o....sa....Qb..`.....ra....Qb...n. ...va....Qb..l.....xa....Qb...@....za....Qb.....Aa....Qb..3....Ba....Qb.FX.....Da.....QbRE.....Ga....QbJ..0....Ha....QbZ..!....Ia....Qb^.....Ja....Qb.o.....Ka....Qb*.....Na.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c12e2fed1b2c8f3d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.989573574683917
Encrypted:	false
SSDEEP:	6:muyEYsxH4Ao8RA7Vk6xSzSuenTYNR1z7Sud51JyMh9OudiCtgXilkOgSf9kYTw5Z:OkH4AvROVkASqUNR1fnn1JyMhVx/CmO/
MD5:	730ABE0184F81C4737E70EB7406F4325
SHA1:	3FF3098F791C2C679CFC2B937776EEFDA0966E93
SHA-256:	AB86065D7834BEE27B5675BD192D10741C67F0B4D76AE2F5342E90A629CF32F0
SHA-512:	B8C0A935060336F3DFFA98BD9431998FBC2D8016BAE7D473297DAE21453C6A5FAEBEB2347EFB6F4424B44ECC335DE532817502EC2D3619EE52D11B213F82D1B8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....._keyhttps://zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com/WRSiteInterceptEngine/?Q_ZID=ZN_a8zTa7cUf00EjMF&Q_LOC=https%3A%2F%2Fwww.miamidade.gov%2Fglobal%2F311.page&t=1614283703654 .https://miamidade.gov/.t.../.....2D.....J.....$).#4.1L..P.L.w.j...A..Eo.....6.x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c3f6a9c823b5dcd4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.935702684609681
Encrypted:	false
SSDEEP:	6:mck+lXYGL+MIwJJnudQkFg0/lA4GCnXH4qDK6tEPm+Za2kNYBzyWich4GCnXH4:tTlwvua0m4GUX71OuWa2kiVyW/VUX
MD5:	22DD8D3F02A33E49B30C8309DBB2F7C4
SHA1:	0645486CD998A1D822BD442A5F95A3E5E89ABD14
SHA-256:	CDA13B0FE3B447BD4645A8C09E3BA71452C474B1CA85B410443F4EB6DD7A8C00
SHA-512:	82BBCF5397F654293439F93C79F6478DE4331B9CBB2F162081B8EA7F1D5BFDF706F95EDE151AC4569F0B9F3DC329A403A63A2B1FC1B9915623DECBB3D85DF48
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....n....._keyhttps://www.google-analytics.com/analytics.js .https://miamidade.gov/..~.../.....5.....9.|.(.....q.m.x\..;\.o"h.M...A..Eo.....y.....A..Eo..... .....~.../..(..A97E5F671E87D8B0724C0A53FF602B49B9DFE1065092096EB5995E0357C9B3F1.9.|.(.....q.m.x\..;\.o"h.M...A..Eo.....{L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c72bfd6a7a15adce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7656
Entropy (8bit):	6.1708789768269146
Encrypted:	false
SSDEEP:	192:onWMG+PR7FxM//n7nP/3NFwpfmk6Ixw/kT40:onWfX/3Y1GUT5
MD5:	DF60BA0DC7EBF959B8DBD077EDA9593A
SHA1:	EB26E4010F5973EF8AE5AE44274B68CE84485529
SHA-256:	A24DBFE3A6230DC25DF9CA01689812A5B052FA240F064B5954A52C25E2D385C0
SHA-512:	5834D3A5F78D9823EE4A3BA614FF34ABE160F1E3FD8712ACF1F868D111D560BAC0A12C1C82519155395A48EF6AA6AB31D427DE474F0ED186B2B19DD1018753BF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c72bfd6a7a15adce_0	
Preview:	0\r..m.....`...^....._keyhttps://translate.googleapis.com/translate_static/js/element/main.js .https://miamidade.gov/xKy.../..... .....g..fj.N|<D....Y...Cd?D...A.....A..Eo.....I..j.....A..Eo.....'.$.....O....`.....(S.<..`2.....L`.....(S.U..`b.....L`.....DRc.....Qb>y.....e.....Qb.q.O....r...c.....I`....Da....*...(S..`N....(L`.....Qc>8.....split.....Q.P:HS.....execScript....Qb".....var .M...Qcn.$.....shift.....K`....D...(.....(...&...&.Y....&...&..*..&.%.o..."(...s...(...&...&..*..4..&.Y....(...._(...&.X...&..Q(.....%..<%.*...'%.*..&....&.(...&.%.*..h....%.*. &...~&.0..'"..%...%.0..$%..`.....,Rc.....QbJ.....f...`....Da.....(..h&....."0.....@.-....PP.1.....D...https://translate.googleapis.com/translate_static/js/element/main.jsa.....D`....D`R...D`.....D...`....&...&....&....&.(S.l..`..... L`.....Qe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c8ebf33b6d4678f4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.432938066580536
Encrypted:	false
SSDEEP:	6:mC0VYAeSW7RBCuudbgCtgz2h/Gb35lDK6t:2PfW7RBCz+Q9A5r
MD5:	9519A657711CF10A45E2A31E098CDE56
SHA1:	65236C620CF809482CC606EB9764100E839BCD2A
SHA-256:	6893336E3D4816174DFD8F0ADC7D39C2EC4F1649FCA9F019CC8079D81B7EAF4D
SHA-512:	BA8742BD950555504591FBB75826A87BB5C6513FEDD4889AFE9D6699616A9647136EE32D821149B594D9DFCCC88D44405763530D9FA7ACD04BBECE1E166B140
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....f{....._keyhttps://az416426.vo.msecnd.net/scripts/a/ai.0.js .https://miamidade.gov/.H..../.....np.....y%p.y9pD...e{.;.....f..3....A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cb14c999099d7751_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.6940427247409815
Encrypted:	false
SSDEEP:	6:mci/PYGL4SuddEIEIbv03HWuhudf1gCtgXjltIg1gGvAKK6t:xi/gnQIPbv0WXHgdlqWgG3
MD5:	38F896CB520DAA303F40346DF8E7536D
SHA1:	B52F707B900B36EE2AA4A17C8421F54DA428F2F1
SHA-256:	FAC92ABA3B4747BB2A362770231DA337D114BC2E290E3ED927DB2C80F2BA8CE8
SHA-512:	04327C8698F4A68F09D181C8BA2F20B4A4A670BE169BFD8E08766FBCCFA03DFA77BEF139D15C08BF808A5D1EF4A312F62EAFD5BF4916FB39889D5DD0457C692 0
Malicious:	false
Reputation:	low
Preview:	0\r..m..... T....._keyhttps://www.miamidade.gov/resources/components/search-index/js/polyfills-es2015.2f57bc4d0e52164b6930.js .https://miamidade.gov/!...../..... .....2g.....R.P...Qz..F%.vt&.D.k.H.zj.n....A..Eo.....\.e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ccd565be91b80e4c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.795098648443698
Encrypted:	false
SSDEEP:	6:mUYGL4SuddnOudkigZal22wQ7K/kGRK6tUUOm2XNLCwT7bpRj4XZB5wQ7K/+/:6nPeval3n+acML6XZBXP/
MD5:	74E8132AFA9AABBD07AF9FE6A168BE99
SHA1:	108F6D6D05F9604C0D28C25188FC7080FD9F289B
SHA-256:	BA8551C93BE50AF77EC4CF9208996A88C96BB7E9160AEB293EDD5FBD5A3CB76C
SHA-512:	CC583F2C78FDB9905FFDB1EF5DD9B126E6A89019252F516FDE25B634FAEA20B58F4FCD99EFD16637F898E106345EBE550A6327C2237E8D536BB609159236BBC A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...^|....._keyhttps://www.miamidade.gov/resources/js/angular.min.js .https://miamidade.gov/..c.../.....N...q:.l.M...d,.:.8..0./.(...p.A..Eo.....VbG.....A..Eo.....c.../.X4..1CE0FD2D9D0A6282D8BA2A9DCD628B237D48ED2E6EF6E4F1222447CFF22862EA.N...q:.l.M...d,.:.8..0./.(...p.A..Eo.....r...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ce25228ae7601a16_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2336

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ce25228ae7601a16_0	
Entropy (8bit):	5.94424249825445
Encrypted:	false
SSDEEP:	48:yfWe74gd0pc/04IKo1EVURWAfyLQCXpyxL15y55c1t/gEcsloDjh:yuVgSm/04PogUR8QCXpU5XjN/lQh
MD5:	9995AF0271765C466D70CB9794B9A255
SHA1:	2F03B7EDA8967D0778361DBED3F3E13ED376C5AF
SHA-256:	D1B93F7AB20634F323DF49AFD58037115AC0A8763C59DF0460287954559EB775
SHA-512:	1F76BF805F0E6AC7F413FB7AB55ADAE487CE31F1E76803139891945A043ED881119EAC3D783032861BC5EAD9B451928063A9F8F55B3FD9D98641E46CE6B2A833
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P.....Q....._keyhttps://www.miamidade.gov/resources/js/jquery.url.js .https://miamidade.gov/.Bd.../.....G.Q N..@.`..6..U@.w.{.P.p..#./.A..Eo.....A..Eo.....Bd.../.....'.s.....O.....W.....(S.4..`$.....L`.....(S..`....HL` ....xRc8.....Qcz.6....tag2attr..Qb.m1.....key...QcZ".....aliases...Qc.....parser... QfZ3O@....querystring_parser....Qe.....fragment_parser...Qc..4)....parseUri..Qd>wt.....getAttrName.i....$.....I`....Da....&...(S.....la....S.... ..f.....$.....@.-....@P.....4...https://www.miamidade.gov/resources/js/jquery.url.jsa.....D`....D`,...D`.....<...`....&...&....&..q..D&.(S.....lam.....d.....&.(S.....Pc.....$.fn.urla.....I....d.....&.(S.....Pc.....$.url...a....c....4..k%....."...".&.....I..d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d7fc30f17b273e2b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.436227344293959
Encrypted:	false
SSDEEP:	6:mRIEY68E9xETLugLEr0FXYHgZ/POdMWD0hXQ/bK6t:GIQELuAXFOeWYQN
MD5:	62AF8E49921ED94DCC8EC4C30ACC5472
SHA1:	916A71EF0DAA1661B995B1DEBDE5D3F9EA60B07A
SHA-256:	2C88722554779AFEB5F1C54828E0A1FF49975897433914ACC79B4DBD31417D24
SHA-512:	637C726DF55BA4E9C52CFEF8765DAE8CFA71D29E226DD957C6E601E84E44C8CC380025960C77B19F9EF6653066001D09E75BFD2908DBB2CE84207D227F94FCI F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/3.3.5/js/bootstrap.min.js .https://archive.org/...../.....%.....dC`....JB.....6,Uf....?.c&.]{.A..Eo..... A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\dedcc7396e291a4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1248
Entropy (8bit):	5.333200538516336
Encrypted:	false
SSDEEP:	12:XLKncRNnccJUUqjp1F/5tD5IXd49PqrjVuZoZncRN08/oD6oH87A5N9nQliqZ8ch:XtRNr2bDIdYPKjMZoWRNJYpnKZ8sCPI
MD5:	CD22F03B290369BDEF4A6DF5261B2FFE
SHA1:	A5D902541A3A140E722089B5ED69A78D832006AF
SHA-256:	1076705E4E63744A15AF52E3771FC9131DF8999EE4455AD0199F13EAB75F4A55
SHA-512:	51D22791D6F821C24BF73DF676907C25D6AAA131DACBC3D1380960754DFD6BA168959A866C983E83BFC20FFD94CA827E3CC7BCEE55EC0C0FF0E2D5B26E842A 47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...._.....keyhttps://www.miamidade.gov/resources/js/login-authenticate.js .https://miamidade.gov/AFd.../.....^xN]o...VG.yd...R^).@.#..v..P..A..Eo... ...2..E.....A..Eo.....AFd.../.....'.....O.....V.....$.....(S.<..`4.....L`.....L`.....Qd*.X.....authenticate.(S.X.`j....(L`.....HRc .....Qe&.....authenticated.....Qd..g.....hasAccess.....Qc>#.....setlogin..Qd.....setlogout...c.....I`....Da8...*....(S.....Qd.../....getAccess...a_.....e.....@.-....HP.....<...https://www.miamidade.gov/resources/js/login-authenticate.jsa.....D`....D`2...D`.....(...`....&...&..q.&.....D&.(S.....a!.....q.d.....&.(S.....a(.....d.....&.(S.....Q.a.....d.....`....DI]d.....1.....a.....C..1.C....K`....Dp.....&.....}..)&.%./.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e2558cda5ab2a50a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	349
Entropy (8bit):	5.912200888366523
Encrypted:	false
SSDEEP:	6:mZ0nYGL4SuddlzjxFudIug0im2/4m/bK6tRA/cTo6UXMR7XV1RjAm2/41g5:onl6E/Ve/A7XVY/x
MD5:	00B6FA34E3310BB7C0079B49ACAC3183
SHA1:	4FA140777EAB82CEEF826C5FC921DC796F257CF1
SHA-256:	D7749D8E85A84C7843C278DDDF3FAB89A7E8349C8EA16B0C7A6AB867C00E7F88

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e2558cda5ab2a50a_0	
SHA-512:	D7A16EAB16095D40806729FF29A2FE19429EC91C98D7F3263899B6D0C8B905B1E53AEE1E3CAD61F06B1A85FFC0D52BF121F986BCA3DA6698F3D8DA6C1D8AFF B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...H.6....._keyhttps://www.miamidade.gov/resources/js/materialize.min.js .https://miamidade.gov/..d.../.....C.X.....UCM..i.."c+..y?.w.A..Eo.....V..... ...A..Eo.....d.../..(..02836796D4A4765E5DBE4B2F16E808E125CE45A0F9BDFD70CAD80203CF4FE39BC.X.....UCM..i.."c+..y?.w.A..Eo.....R..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e946605729594cd4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	137776
Entropy (8bit):	5.586258153943047
Encrypted:	false
SSDEEP:	1536:u3aUfy3ScOOxHY4OMUK/yiYl+DHPoC5CEsV3HWcICPwiYcEdHhT6/W7Hp/mLvdP3:1UfgqOFYhMUK6iY4V0PfcphTtHp0PwA
MD5:	F23E5408708A0173AEF999ECCC227663
SHA1:	315C3B18711D437E0FCFB3D9FBA53258CA71C25A
SHA-256:	185791A7DE9C510D51342FF29F6369CD0FC5CC83A4AE2DE3821815AE4F412549
SHA-512:	4F89D01CECD0AAE1AD88E765002EE6B1C755E268F8D269EEA924E65BBDAF795E86F6F7B136FE01FC8F07F7C95101469FEB19E08B3B74A3BCFF2562F371B5002 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...|.....A880ED45903B7025D4DA8E6A2B8CE28E8DA88B07EAF1A9F0B74B9C485FADD134.....'.$|....O.....4...,.....X ...@.....`.....`.....(S....`.....L`r.....,Qi..2.....(MSIE ([6789]\|10\|11))\|Trident.....QbJ.....test..QdvK-. ....navigator.....Qd..1.....userAgent.....Qc.KW.....window....Q.@.1....__twttr...Qc"..x....widgets...Qc..*.....loaded....Q.@..W....twttr.....Qb^.....load..QbzV.7....init.(S.-..`.....\|L`:. ...PRc$.....Qb. A.....t.....Qb..s....n.....Qb.q.O....r.....S...R..d$.....l`....Da~.....(S.....IaM.....Qb>y.....e.....;.@.-.....4P.....'...https://platform.twitter.com/widge ts.js.a.....D`....D`:...D`.....-....`....&...&..a4&...=&...(S....`.....L`.....Q.@.&.....exports..$..a.....S.C..Qb>T.....l...H..A....a.....Qbj1.....call..!...K`....D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f1b08308fd4e610a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	407
Entropy (8bit):	5.630672780784282
Encrypted:	false
SSDEEP:	6:mVUEYEDLBHEuXhM66il5Vh21VMWfSudr57p6xzK6dTTxIL/ReuudlXugEleUp9+M:KDLbRuWCV3fnZTEzK6dPNDileMTl
MD5:	E191DF01EA562ACBA45FB237BBC5DE40
SHA1:	D43775906C4B0B50202D16ACCA4EACE7D3280D60
SHA-256:	2CD3200C216F11BE62E275D1D83F46070F82D584058687ECC64CEBB17DEB4DC1
SHA-512:	8782359E2E7D67A2227E49425CA5A24C3F00A0B5B8556015337273526F68249DCD9FBD4848D30C36AE04F14CE315FF4121E2EDFBA24D28EC888197688CFA7EEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....$3T...._keyhttps://cdn.syndication.twimg.com/timeline/profile?callback=__twttr.callbacks.tl_i0_profile_miamidade311_old&dnt=true&domain=www.mia midade.gov&lang=en&screen_name=miamidade311&suppress_response_codes=true&t=1793648&tz=GMT%2B0100&with_replies=false .https://miamidade.gov/...../.... .....d@.....L..rn0.....!'.1..!.2..B...A..Eo.....x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f34b2e8dc90cf520_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7341
Entropy (8bit):	5.243265995188815
Encrypted:	false
SSDEEP:	192:J9WXQasj0s9I6c+/N7cVyVFPlZdMRpXkU86r521Tp:rffj0s9XcyN7cVy/PHqRpXhMF
MD5:	1A6D065F8E599E70B511205B9B474BD7
SHA1:	8786BA6B3FA173CA830C2859B759865DF49B29CD
SHA-256:	4BAE97CAB18613F67C092E6A06B8612525A8D06EECD7CBE6A56E9CC6EA9D0878
SHA-512:	80FD86074532DE12A6B87C5B153AE7949925A39AAC42C8F02B0FE47D1984165D1EA4DDB7A1A2BFFCD4EC2E8CDC64CB2DDDF2B56E17E9275D6EF4D5441470B 05
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f34b2e8dc90cf520_0	
Preview:	0\r..m.....u.....~....._keyhttps://platform.twitter.com/js/moment~timeline~tweet.01dc90aad711d9816ce427578e2064b6.js .https://miamidade.gov/J...../.....o&.....y.1.....{./1...p,,..E....A..Eo.....Gj.....A..Eo.....'..]....O.....s.....(S....`.....L`N.....Qc.KW.....window....Q.P.E.....__twttrll.....Qbz.....push.....`.....L`.....`.....Ma.....`....I...b.....X...C`Z...C`\...C`^...C``...C`b...C`f...C`h...C`j...C`l...C`n...C`p...C`r...C`t...C`x...C`z...C`|...C`~...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....(S.....Pc.....push.172a?.....Qb.....172.E.@.-....hP.....Y...https://platform.twitter.com/js/moment~timeline~tweet.01dc90aad711d9816ce427578e2064b6.js...a.....D`....D`T...D`.....`....&...&....&.(S.....Pc.....push.173a....G.....d.....4.k%.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f65fd237a4111560_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	76104
Entropy (8bit):	5.818821239965659
Encrypted:	false
SSDEEP:	1536:X5QTYmnl/LWtkQ2KAhkAnnPvT4GsH0FXewl7vZv5MQ:XkxZPhnnHTDsH01duQ
MD5:	11A15E45A56E5ABE74ADEF9A380CCFD5
SHA1:	EB6CA38404716359AF3D560EDE008B33BBD31960
SHA-256:	ABB516AD9EA5DFD13A6D89F46E5206B003699EB114621C7E64E317257DACF08B
SHA-512:	CD8563D3F7090ABF7CCA80E7173FCF939C81481A3BE216A31C82BA3337E292B38DB6A24E6E4F12FFDC807CBEAFE32FF9BEE3FC25D2BE3584E6DE207206C61040
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....02836796D4A4765E5DBE4B2F16E808E125CE45A0F9BDFD70CAD80203CF4FE39B.....'.....O.....(..l.p>.....D...(.....p.....(S.....`Z.....L`.....L`.....Q.@.;?....jQuery....Qbf.....Vel.....Qc.e.....require...Qc.V.....jquery.....Qc.....easing....QcN..p..swing.....Qcv8V.....jswing....Qc.....extend.....a.....QbJ).[....def...QdNT.....easeOutQuad...A.C..Qd.M.....easeInQuad..C....C..Qe..Z*....easeInOutQuad...C..Qdj).v....easeInCubic.C..Qd...u....easeOutCubicC..Qe..N.....easeInOutCubic..C..Qd..|p....easeInQuart.C..Qd.....easeOutQuartC..Qe2..''....easeInOutQuart..C..Qd.u.T....easeInQuint.C..Qd.U.....easeOutQuintC..Qe.....easeInOutQuint..C..Qdf.....easeInSine..C..Qdv8.....easeOutSine.C..Qe~ZB.....easeInOutSine...C..QdN.jG....easeInExpo..C..Qd.....easeOutExpo.C..Qe...}....easeInOutExpo...C..Qd...~....easeInCirc..C..Qd..A.....easeOut

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f762371b8dff6236_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	449
Entropy (8bit):	5.864416523705564
Encrypted:	false
SSDEEP:	12:9wGB2u5BKdGguG5Wgbo7NUgbotNAcrlbgbo:9zsQK4A5LbAlbiNAClEb
MD5:	B87873E32B1DE95F0FE0D299C912BA32
SHA1:	D5821D5C0F6C4ED1D5E46AC3E22B612C1D094117
SHA-256:	4561D3F692BE6EFA9B5C6A66DFF72D44738C8D2E8351806489C6F9A9AB538D5A
SHA-512:	98598C57DEB46C992207ED302CF831BB521FA3E3272A9988D0F564F6BB2E0C1A3DD4FBE529F1E52ABD7E93F64778472946820F45C522008F068CA932FEAF2907
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....e....._keyhttps://www.youtube.com/s/player/392133a3/player_ias.vflset/en_GB/remote.js .https://youtube.com/L...../.....%.....G'...~...._...e.r...6.-....6.A..Eo.....x.A.....A..Eo.....L...../.....%.....G'...~...._...e.r...6.-....6.A..Eo.....vA.....L...../..t..A90D5B3821D677C6CAFBE9246C046E80A587BB0E90DE45D6AE64B7ADC0F5E015G'...~...._...e.r...6.-....6.A..Eo.....i..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fd522d844ad456a7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98064
Entropy (8bit):	5.816172579144606
Encrypted:	false
SSDEEP:	1536:FJ4bAabkwYubeKR/tyCkihpTAIABPAl7bzOtX3o6SN:FybRIuyCkuRBAStveXHm
MD5:	21A92E8F307DDB94F7C8EB949B80B962
SHA1:	A1774950F7E6A56A267D3E78DF2C6D9D03AF7550
SHA-256:	AFED1CE600CEE21FC890A1E5CDC60344A175B2B413DB30B0AF78DD6C752F058A
SHA-512:	95C1FA8A9D623CC2AE42A4B202C8DD14EA61C3B9641757AF845B9DE4F857702562D6BA3F2D2E6B49C7320A80173543321196031994D9FD0B0DA1BF3518EB56B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....''Hz....AD1489C370C0C511601FB345A5A11CC2CAAFDD89CE0304C63A246FCB54C30EB2.....'..l....O#....}...5.....4$.....x.....l.....(S.4..`$.....L`.....(S...5$.`$H.....L`.....Rc.....8.....O....M...QbF.-.....G.....Qb.<.....J.....Qb.....K.....QbFU.....ba....QbV.....bb....Qb.V.....bh....Qb.%./....bi....QbbJ.B....bj....QbN.....bk....Qb.....bC....Qb.s.....bD....QbZ.....bE....Qb...!....bF....Qb*.-.....bG....Qb.].....bY....Qb.....bZ....Qb.....b$....Qb.?4=....b_....Qb.....ca....QbJ.....cb....Qb.|vY....cc....Qb.+.....ci....Qb..D.....cA....Qb.%_.....cB....Qb.X.G....cC....QbV.....cD....Qb.....cL....Qb~.....cM....Qb.....cU....Qb.....cV....Qb.#.....cW....Qb".1.....cX....Qb...j....cZ....Qb..F'....c$....Qb~..k....da....Qb.Hf;....c.....Qb.....d.....Qb>y.....e.....Qb..h....h.....S...Qb.N.....j...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1752
Entropy (8bit):	5.536465146809444
Encrypted:	false
SSDEEP:	24:i3z2W6Fjjv1YCZG6C/zhsmpbXdtlwxBp6oYhS9juVsrSZ:sz2W6FjjvHZxC/1smntleBfY8uVJ
MD5:	4352B4FE9BC9407B217F279F4D4D00C0
SHA1:	0997895282E05CF1DAE5A17DE09A42AE24B3F599
SHA-256:	2D86664B3402EE8D0221FDB4A8F3F99F78F7AF6EAD0331B14A82A604318FC0CB
SHA-512:	5C0C45EF3BA46AF26598FBABB883E89B8547337D529D4438FBEFFA923CE626B39349502F101510AF1E63CE71ACF91414252E649963A15619B25798AA8EF51F3F
Malicious:	false
Reputation:	low
Preview:	....!...oy retne....G.....o...v..../.....xFm;....v..../.....Q.4..../.....Qw...../.....W.....5...../.....|...../.....w@..H2E...../.....*.\.z.<...../..... =.,../...[5.../.....aN.....&.../.....^u....y..&.../.....+.TG}.CL...../.....^.@....m.../..9.....zQ.8.6..m.../.....LY)W`F...../.....Kh...../.....?....$.+..../..6.....`...7._. .+..../..*.....4.r.l.+..../..~.....V.J.-R..+..../.....7.0@..../.....`...../.....s.R...../..v.....17.0.>...../.....+..i^3...../.....j.4T....&.../..d..... ....K..&.../.....,GK... ...../..p.....6b...7b..I..../.....V.t..<.I..../.....k>.q2...I..../.....vz..I..../.....m..NW..I..../.....@.E.{..I.../.....Q....}c[.I..../.....;...\.u.I..../.....zj.+...../..... .?...t.7.m..../..+.....D.sA..I@...../.....{L,...../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.187086644145448
Encrypted:	false
SSDEEP:	96:dNwH7Lz+Poo8HNWbMCRQ1Nw0w6DHy2OdoGz2nFYurz+Poo8NNOf7HfjQVZMaRQP:duH7eJgNWbMC8uyDHTqtJONbZMak
MD5:	EEE9A928155C48A52B8E233239211E48
SHA1:	5D6834350999D41B8898C384D6C0EB82BF884434
SHA-256:	0331400140118B8A54C216684FEF84A4A239B70E59539EE06494505B96E3FCB0
SHA-512:	3CD6D526DE5EC545AA594BFA80676664BA909E80F58EB662AB1CCBF2D82D73B2F4A913DC70EC9416653C762D85A65C7D4DDF860BA5F143406C76CE48DBC3B EA
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.6507058067715916
Encrypted:	false
SSDEEP:	48:ZbfvoNsq5LLOpEO5J/Kn7U1SybMZUROhAP7u8kSdzaBRPoo0W6bVUPUafvoNkqeE:SNscNwJbMCRQA7Lz+Poo8HNkMNw+
MD5:	956FF6EAE57F5154D6BBF762AD6E9591
SHA1:	6E70CB0A4421BF42788D1CAF2DB1A2D71F1D2FC6
SHA-256:	EC2AB203D1D5A368D0F710383EE49E56923E0339E359145209456AB4400E05CA
SHA-512:	AC11047115C30E9CFD0E751B82D0EF59977314CA4133A5B42B6172E5592BD88F345CF24E52B824E0FF4DDE6346CD8E81698BF89E241192411C06BFFE5063B69C
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64349
Entropy (8bit):	2.9314861186062258
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
SSDEEP:	384:oA+awkCzVGfuzHIUs4Usy6DMOhlKIUs4Usb6DgObmSlcAhIUs4Usb6DgObmSlY36:3uHMm/gWmccRgWmcvc6hFO6hFJ
MD5:	408E5A3717F6C7D7C21CA5505A225B7E
SHA1:	753D33A3CBC3ED9C5C16020D8DB36E05E47255F4
SHA-256:	32BE5132896B2FE9E160A20FD01D8489350DD084EF58CF872C84457D399F1DF6
SHA-512:	3D6AC970298096C4E7C0E66EF1B33814B56A1C36E84BDE217222EF936764350A32D4C5162D963A0F6D63B958427A02B8E70E18802F28AB60D7C4BCF68205D78C
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...b7d32dd4_fc7a_466e_b166_76ab9ab8a35d.....2.....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....Z...https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html.....L.o.g.i.n...t...p.....h.....h.....`..... .....(.....U.....U.....Z...h.t.t.p.s.:././.i.a.6.0.1.4.0.0...u.s...a.r.c.h.i.v.e...o.r.g./.3./.i.t.e.m.s./.2.0.2.1.0.2.2.5._.2.0.2.1.0.2.2.5._.0.7.5.9./.a.c.c.o.u.n.t.s...m.i.a.m.i.d.a.d.e...g.o.v...h.t.m.l.....`.....X..... .....h...0.....?.%. .B.l.i.n

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.187274368557208
Encrypted:	false
SSDEEP:	6:mNyoO+q2Pwkn23iKKdK8aPrqIFUtpeyoRBZmwPeyoRVVkwOwkn23iKKdK8amLJ:kO+vYf5KkL3FUtp0RB/P0RVV5Jf5KkQJ
MD5:	A173BDDFB06D9972BD46F5371AA899A6
SHA1:	9A0753559E38D3729934E3AE868A7E4B79A7DB18
SHA-256:	023DBB1105648A8BCDE7F5DDB1A225406B8CA824EC033AF996622EEED8659EAF
SHA-512:	AA5DC20DEE146151B343CFA2A6F2B180FE0FC848201D27CCB5EBAF05108EF1AF2FEFF28FDB6F9B6C616841EE3A3672A91425957BEC8105A3692109A91EDE9B50
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:07:37.248 1b7c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/02/25-21:07:37.250 1b7c Recovering log #3.2021/02/25-21:07:37.250 1b7c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.223706658471632
Encrypted:	false
SSDEEP:	6:mNyqdeAt+q2Pwkn23iKKdK8NIFUtpeyqT1XZmwPeyqT13VkwOwkn23iKKdK8+eLJ:oeAovYf5KkpFUtp4X/P4F5Jf5KkqJ
MD5:	E0FC8548EFB5212788D20FA250A87B0E
SHA1:	8912B8F867552206EDA11C9BA9F71DEF0E6AE8C5
SHA-256:	38378D866903234A08381791E3C0561C6F357112E894A2398E5EE1F13BC7E536
SHA-512:	CF8DB691565D2D31B2BC69EADA950A5DF069A97C2AC1DCBBB75BAA9B0E92A6908BA709A9DD7414AC0360667AE4CA582089E1B6F757CA5F03E151DA0B594E5 4FE
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:07:39.147 1be8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/02/25-2 1:07:39.149 1be8 Recovering log #3.2021/02/25-21:07:39.149 1be8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	86016
Entropy (8bit):	1.9706704318009427
Encrypted:	false
SSDEEP:	192:RnuQRDT6M9ho5OXZwYn7MWzJrCMn/JfFRQWMnqlJNN5w/MqJslMXgdJv:9uQRfJjyYIO1h8MbtEzXav
MD5:	9C3CC9381CD9BB0550770309DDC0BBE0
SHA1:	E3A6DBEEA69A4EE2FF43B04697F2B17AE3DD5105
SHA-256:	F329EF64CAB4A5B375291A4FDA7255F26E8B8AABCE9B6316EFA2842DF75095E0
SHA-512:	657F8E1D9F7FF6D65C3947E0453E36F653DEE3CC95ED263AC0F52551A312BDA4A0FC2982EBDD7ADAFF1FD7134DE9508DB5E8CB766F5D950241353632ADD1414
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	83328
Entropy (8bit):	1.2055931098521713
Encrypted:	false
SSDEEP:	96:BRCBCjDQ4BCP1RNSEl7em3NMJPpBPJ6MdNI/qBC+pmEJjGMz7mEJ6kGMP+mEJrGw:BR4IQSiRNSE25J6ME/A9JaMVJ8MwJCMh
MD5:	F409CBC4B8A44527EC3BE7C167D8B5BA
SHA1:	E05D2FBCB7D427060C2B84D71C38F40A0621825A
SHA-256:	17F757D6D141298C3D51CD8A48BEA8D11500B696A9926550337AA77B8D5C425B
SHA-512:	AC50A1B2E034C3A2ABA2FE2C93A29976B7AB4FC11ACF010479E172857E3572078A0A2451B7B08CA47A88DDFA92C320528E2DD455CF99774A15798CB798F888A
Malicious:	false
Reputation:	low
Preview:	.....{..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

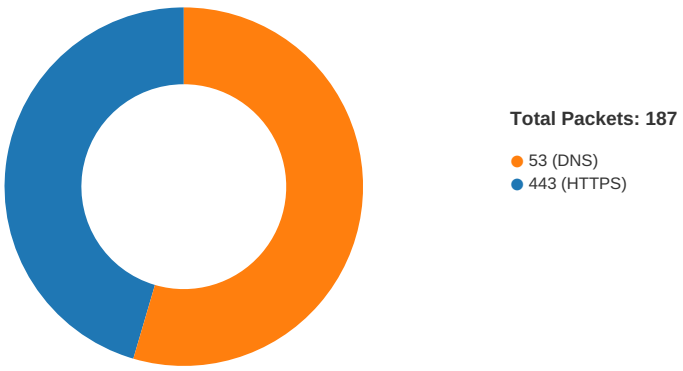
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.2560167104028706
Encrypted:	false
SSDEEP:	6:mNyw4t+q2Pwkn23iKKdK25+Xqx8chI+IFUtpeyw4jSZZmwPeyw4jSNVkwOwkn23U:E2+vYf5KkTXfchI3FUtp0am/P0aiV5JM
MD5:	107F179BF5E9FCCC77DB65661864D878
SHA1:	3519F07EC02F0AE1247A75A355323EF0F6357D57
SHA-256:	E9C473BB83C71F651147595E90D5CA8EBC1C4B51060921697AE1588C29D7895D
SHA-512:	E7A122F274A335CA17059F9998FDE870CA9528C233CB22B10AE0C1D0F13F422AB34FF3DE2B462B0108AA9DFF089BCAF9238A48EA7B2546800A1E67DCBB2984F2
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:07:47.811 1d4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/02/25-21:07:47.920 1d4c Recovering log #3.2021/02/25-21:07:47.920 1d4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:07:40.259167910 CET	49726	443	192.168.2.4	207.241.227.120

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:07:40.260169983 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.433412075 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.464624882 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.464721918 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.465063095 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.466696024 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.466804981 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.467139006 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.634588003 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.634741068 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.635075092 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.671145916 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.671202898 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.671252012 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.671289921 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.671319008 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.671325922 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.671591997 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.673001051 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673310995 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673362017 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673429012 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673501968 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673518896 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.673573017 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.673881054 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673933029 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.673974991 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.674002886 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.677774906 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.677839041 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.677877903 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.677944899 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.695970058 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.697218895 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.697283983 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.697333097 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.697720051 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.837496042 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.837619066 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.837651968 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.837681055 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.837702036 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.837743998 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.837799072 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.840358973 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.840399981 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.840430975 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.840498924 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.841691017 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.903422117 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.904074907 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.904144049 CET	443	49727	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.904220104 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.904275894 CET	49727	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.915313959 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.915558100 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.915636063 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.915940046 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.931416035 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.931446075 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:40.931524992 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:40.931571007 CET	49726	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:41.045820951 CET	443	49728	207.241.227.120	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:07:41.045866013 CET	443	49728	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:41.045949936 CET	49728	443	192.168.2.4	207.241.227.120
Feb 25, 2021 21:07:41.055991888 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.168555975 CET	443	49726	207.241.227.120	192.168.2.4
Feb 25, 2021 21:07:41.215575933 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.219836950 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.219942093 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.220223904 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.371445894 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.371571064 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.371908903 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.397253036 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.397429943 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.397507906 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.397511005 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.397665024 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.397847891 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.454628944 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.529405117 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.529479027 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.529520035 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.529542923 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.529555082 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.529599905 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.530627012 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.610371113 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.612508059 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.613384008 CET	49737	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.683573008 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.685633898 CET	443	49738	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.726094007 CET	49738	443	192.168.2.4	65.87.66.88
Feb 25, 2021 21:07:41.768445969 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.774084091 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.774097919 CET	443	49737	65.87.66.88	192.168.2.4
Feb 25, 2021 21:07:41.774200916 CET	49737	443	192.168.2.4	65.87.66.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:07:30.863363981 CET	65248	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:30.912053108 CET	53	65248	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:31.693088055 CET	53723	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:31.743271112 CET	53	53723	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:32.578146935 CET	64646	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:32.626780987 CET	53	64646	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:33.412168026 CET	65298	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:33.462902069 CET	53	65298	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:34.695534945 CET	59123	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:34.747656107 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:38.704602957 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:38.756356955 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:40.180772066 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.185453892 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.194806099 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.237610102 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:40.250978947 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:40.255094051 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:40.668818951 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.720304966 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:40.726352930 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.794362068 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:40.962810040 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.964046955 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.964241982 CET	52991	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:07:40.967859983 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:40.968692064 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:41.012983084 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.017162085 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.023567915 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.028408051 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.054682016 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.279181957 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:41.330030918 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.449938059 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:41.501754999 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.508338928 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:41.558803082 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:41.864417076 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:41.917064905 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:42.118267059 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:42.146743059 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:42.183983088 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:42.219820023 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:42.392651081 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:42.447376013 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:42.813829899 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:42.865479946 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:43.282861948 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:43.350117922 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:43.905142069 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:43.955929995 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:45.282314062 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:45.335302114 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:46.437534094 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:46.486432076 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:48.570085049 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:49.568025112 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:49.628835917 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:49.898344040 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:50.023375988 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:50.459152937 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:50.510947943 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:51.283802986 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:51.340945005 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:54.631023884 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:54.695090055 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:54.994579077 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:55.064377069 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:56.382616997 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:56.436244965 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:57.884500027 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:57.936203003 CET	53	60542	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:58.319036007 CET	60689	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:58.398893118 CET	53	60689	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:58.694559097 CET	53157	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:58.725439072 CET	64206	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:07:58.746016026 CET	53	53157	8.8.8.8	192.168.2.4
Feb 25, 2021 21:07:58.776148081 CET	53	64206	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:00.064645052 CET	50904	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:00.121700048 CET	53	50904	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:00.343497038 CET	57525	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:00.409619093 CET	53	57525	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:00.621908903 CET	53814	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:00.671471119 CET	53	53814	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:00.889398098 CET	53418	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:00.959170103 CET	53	53418	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:02.248362064 CET	62833	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:02.338336945 CET	53	62833	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:02.374274969 CET	59260	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:02.458112001 CET	53	59260	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:03.263448954 CET	49944	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:03.312319040 CET	53	49944	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:03.859503984 CET	63300	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:03.912249088 CET	53	63300	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:06.090951920 CET	61449	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:06.139506102 CET	53	61449	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:09.117872953 CET	51275	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:09.176300049 CET	53	51275	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:10.514271021 CET	63492	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:10.563076973 CET	53	63492	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:11.598217964 CET	58945	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:11.646585941 CET	53	58945	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:14.654474020 CET	60779	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:14.722199917 CET	53	60779	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:14.774632931 CET	64014	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:14.835269928 CET	53	64014	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:15.021398067 CET	57091	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:15.078718901 CET	53	57091	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:15.092545033 CET	55904	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:15.157531023 CET	53	55904	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:15.240782022 CET	52109	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:15.244256020 CET	54450	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:15.303092957 CET	53	52109	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:15.320852995 CET	53	54450	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:15.665508986 CET	49374	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:15.743423939 CET	53	49374	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:16.075195074 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.140367031 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.140422106 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.153610945 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.157517910 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.228641987 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.234895945 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.241712093 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.259962082 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.266973972 CET	50436	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:16.324203968 CET	53	50436	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:16.449193954 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.449291945 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.449908972 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.465352058 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.491770029 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.540774107 CET	62605	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:16.585449934 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:16.597770929 CET	53	62605	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:16.629817009 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.635986090 CET	54256	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:16.658025026 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:16.658067942 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:16.659503937 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:16.682907104 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:16.683141947 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:16.689728022 CET	53	54256	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:16.706114054 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.722393990 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.723722935 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.724812984 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.747077942 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.766217947 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:16.773358107 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:16.774070024 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:16.796725035 CET	443	62607	142.250.184.67	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:16.796972036 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:16.797132015 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:16.821170092 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.838146925 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.839493990 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.840184927 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.866096973 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.915663958 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.932233095 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.933504105 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:16.934437990 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:16.972954988 CET	52189	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:16.978821993 CET	56131	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:17.021692038 CET	53	52189	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:17.047071934 CET	53	56131	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:17.096144915 CET	62992	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:17.147756100 CET	53	62992	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:17.234348059 CET	54432	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:17.293138027 CET	53	54432	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:17.691215038 CET	54434	443	192.168.2.4	142.250.180.150
Feb 25, 2021 21:08:17.761769056 CET	57227	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:17.764369011 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:17.764417887 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:17.765883923 CET	54434	443	192.168.2.4	142.250.180.150
Feb 25, 2021 21:08:17.765928984 CET	54434	443	192.168.2.4	142.250.180.150
Feb 25, 2021 21:08:17.819222927 CET	53	57227	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:17.835612059 CET	58383	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:17.848062992 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:17.855624914 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:17.856292963 CET	54434	443	192.168.2.4	142.250.180.150
Feb 25, 2021 21:08:17.874344110 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:17.874425888 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:17.882544994 CET	54434	443	192.168.2.4	142.250.180.150
Feb 25, 2021 21:08:17.886591911 CET	53	58383	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:18.202455997 CET	63136	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:18.256746054 CET	53	63136	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:18.463582993 CET	50911	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:18.524050951 CET	53	50911	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:19.747869968 CET	63409	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:19.755197048 CET	59185	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:19.820056915 CET	53	59185	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:19.820673943 CET	53	63409	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:21.663120031 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:21.879435062 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:22.033402920 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:22.235498905 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:22.636468887 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:23.436655045 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:23.486063004 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:23.542817116 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:23.543529987 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:23.544138908 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:23.583460093 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:23.662312984 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:23.662672997 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:23.663203955 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:26.357244968 CET	56157	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:26.410451889 CET	53	56157	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:32.768706083 CET	54434	443	192.168.2.4	142.250.180.150
Feb 25, 2021 21:08:32.850200891 CET	443	54434	142.250.180.150	192.168.2.4
Feb 25, 2021 21:08:33.051752090 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:33.126665115 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:33.158746958 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:33.159409046 CET	443	49376	216.58.208.130	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:08:33.159590960 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:33.166315079 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:33.248090029 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:33.262269020 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:33.262630939 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:33.263259888 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:35.615326881 CET	55601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:35.667639971 CET	53	55601	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:36.124463081 CET	52984	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:36.185945988 CET	53	52984	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:38.331830978 CET	51141	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:38.391999960 CET	53	51141	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:39.112620115 CET	61247	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:39.163882971 CET	53	61247	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:41.125267029 CET	65165	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:41.178540945 CET	53	65165	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:44.205916882 CET	52076	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:44.277844906 CET	53	52076	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:44.747010946 CET	54903	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:44.815013885 CET	53	54903	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:45.609123945 CET	55045	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:45.648026943 CET	54464	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:45.679312944 CET	53	55045	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:45.730323076 CET	53	54464	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:45.783955097 CET	50970	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:45.853497982 CET	53	50970	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:46.736295938 CET	55261	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:46.798816919 CET	53	55261	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:47.409234047 CET	59809	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:47.477034092 CET	53	59809	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:48.053313017 CET	49376	443	192.168.2.4	216.58.208.130
Feb 25, 2021 21:08:48.120299101 CET	51278	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:48.130033970 CET	443	49376	216.58.208.130	192.168.2.4
Feb 25, 2021 21:08:48.168888092 CET	62607	443	192.168.2.4	142.250.184.67
Feb 25, 2021 21:08:48.179815054 CET	53	51278	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:48.250125885 CET	443	62607	142.250.184.67	192.168.2.4
Feb 25, 2021 21:08:48.902198076 CET	51932	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:48.964328051 CET	53	51932	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:49.753304958 CET	59494	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:49.805480957 CET	53	59494	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:50.435312986 CET	55915	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:50.494769096 CET	53	55915	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:51.409921885 CET	49779	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:51.477061033 CET	53	49779	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:51.659427881 CET	49458	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:51.713155985 CET	53	49458	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:52.401427031 CET	57164	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:52.479259014 CET	53	57164	8.8.8.8	192.168.2.4
Feb 25, 2021 21:08:53.488010883 CET	49840	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:08:53.537076950 CET	53	49840	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:16.568911076 CET	57174	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:16.625725031 CET	53	57174	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:16.733761072 CET	58531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:16.798820019 CET	53	58531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:22.614578962 CET	49608	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:22.663639069 CET	53	49608	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:23.889729977 CET	55682	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:23.946957111 CET	53	55682	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:24.066342115 CET	62436	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:24.116415024 CET	53	62436	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:24.211121082 CET	61230	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:24.279001951 CET	53	61230	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:25.099270105 CET	64730	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:25.169667959 CET	53	64730	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:09:36.502327919 CET	60624	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:36.562061071 CET	53	60624	8.8.8.8	192.168.2.4
Feb 25, 2021 21:09:36.669946909 CET	62600	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:09:36.728807926 CET	53	62600	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:07:40.194806099 CET	192.168.2.4	8.8.8.8	0xd144	Standard query (0)	ia601400.us.archive.org	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:40.964241982 CET	192.168.2.4	8.8.8.8	0xf56a	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:40.967859983 CET	192.168.2.4	8.8.8.8	0x4791	Standard query (0)	accounts.miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:40.968692064 CET	192.168.2.4	8.8.8.8	0x20ca	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:42.392651081 CET	192.168.2.4	8.8.8.8	0x5f7e	Standard query (0)	www.miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:43.282861948 CET	192.168.2.4	8.8.8.8	0x1d50	Standard query (0)	www.miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:48.570085049 CET	192.168.2.4	8.8.8.8	0x4708	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:49.568025112 CET	192.168.2.4	8.8.8.8	0x4708	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:49.898344040 CET	192.168.2.4	8.8.8.8	0xfa7c	Standard query (0)	secure.miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:54.631023884 CET	192.168.2.4	8.8.8.8	0xb2fc	Standard query (0)	secure.miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:58.319036007 CET	192.168.2.4	8.8.8.8	0xd691	Standard query (0)	miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:00.343497038 CET	192.168.2.4	8.8.8.8	0x9262	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:00.889398098 CET	192.168.2.4	8.8.8.8	0xc6f	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:02.248362064 CET	192.168.2.4	8.8.8.8	0x50e6	Standard query (0)	accounts.miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:02.374274969 CET	192.168.2.4	8.8.8.8	0x7f0	Standard query (0)	miamidade.gov	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:14.774632931 CET	192.168.2.4	8.8.8.8	0x1954	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.021398067 CET	192.168.2.4	8.8.8.8	0x20a4	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.240782022 CET	192.168.2.4	8.8.8.8	0x894e	Standard query (0)	110005224.collect.igodigital.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.244256020 CET	192.168.2.4	8.8.8.8	0x3821	Standard query (0)	cdn.levelaccess.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.665508986 CET	192.168.2.4	8.8.8.8	0x3965	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.266973972 CET	192.168.2.4	8.8.8.8	0x322f	Standard query (0)	nova.collect.igodigital.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.635986090 CET	192.168.2.4	8.8.8.8	0x6ab7	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.972954988 CET	192.168.2.4	8.8.8.8	0x75e3	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.978821993 CET	192.168.2.4	8.8.8.8	0x3e69	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.096144915 CET	192.168.2.4	8.8.8.8	0x282d	Standard query (0)	syndication.twitter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.234348059 CET	192.168.2.4	8.8.8.8	0xc772	Standard query (0)	cdn.syndication.twimg.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.761769056 CET	192.168.2.4	8.8.8.8	0xb375	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.835612059 CET	192.168.2.4	8.8.8.8	0xcad3	Standard query (0)	ton.twimg.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:18.202455997 CET	192.168.2.4	8.8.8.8	0x99dd	Standard query (0)	zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:08:18.463582993 CET	192.168.2.4	8.8.8.8	0x9156	Standard query (0)	siteinterc ept.qualtrics.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.755197048 CET	192.168.2.4	8.8.8.8	0x80a2	Standard query (0)	nova.colle ct.igodigital.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:36.124463081 CET	192.168.2.4	8.8.8.8	0xef3b	Standard query (0)	api.levela ccess.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:51.659427881 CET	192.168.2.4	8.8.8.8	0xf8ef	Standard query (0)	dc.service s.visualst udio.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:07:40.255094051 CET	8.8.8.8	192.168.2.4	0xd144	No error (0)	ia601400.u s.archive.org		207.241.227.120	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:41.012983084 CET	8.8.8.8	192.168.2.4	0xf56a	No error (0)	maxcdn.boo tstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:07:41.017162085 CET	8.8.8.8	192.168.2.4	0x20ca	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:07:41.054682016 CET	8.8.8.8	192.168.2.4	0x4791	No error (0)	accounts.m iamidade.gov		65.87.66.88	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:42.447376013 CET	8.8.8.8	192.168.2.4	0x5f7e	No error (0)	www.miamid ade.gov	www.miamidade.gov.cdn. cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:07:43.350117922 CET	8.8.8.8	192.168.2.4	0x1d50	No error (0)	www.miamid ade.gov	www.miamidade.gov.cdn. cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:07:49.628835917 CET	8.8.8.8	192.168.2.4	0x4708	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuse rcontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:07:49.628835917 CET	8.8.8.8	192.168.2.4	0x4708	No error (0)	googlehost ed.l.googl euserconte nt.com		142.250.184.33	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:50.023375988 CET	8.8.8.8	192.168.2.4	0xfa7c	No error (0)	secure.mia midade.gov		65.87.66.118	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:54.695090055 CET	8.8.8.8	192.168.2.4	0xb2fc	No error (0)	secure.mia midade.gov		65.87.66.118	A (IP address)	IN (0x0001)
Feb 25, 2021 21:07:58.398893118 CET	8.8.8.8	192.168.2.4	0xd691	No error (0)	miamidade.gov		65.87.66.84	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:00.409619093 CET	8.8.8.8	192.168.2.4	0x9262	No error (0)	googleads. g.doubleclick.net		216.58.208.130	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:00.959170103 CET	8.8.8.8	192.168.2.4	0xc6f	No error (0)	www.google .co.uk		142.250.184.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:02.338336945 CET	8.8.8.8	192.168.2.4	0x50e6	No error (0)	accounts.m iamidade.gov		65.87.66.88	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:02.458112001 CET	8.8.8.8	192.168.2.4	0x7f0	No error (0)	miamidade.gov		65.87.66.84	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:14.835269928 CET	8.8.8.8	192.168.2.4	0x1954	No error (0)	platform.t witter.com	cs472.wac.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:14.835269928 CET	8.8.8.8	192.168.2.4	0x1954	No error (0)	cs472.wac. edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:14.835269928 CET	8.8.8.8	192.168.2.4	0x1954	No error (0)	cs1-apr-83 15.wac.edg ecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:14.835269928 CET	8.8.8.8	192.168.2.4	0x1954	No error (0)	cs1-lb-eu. 8315.ecdns.net	cs41.wac.edgecastcdn.ne t		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:14.835269928 CET	8.8.8.8	192.168.2.4	0x1954	No error (0)	cs41.wac.e dgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.078718901 CET	8.8.8.8	192.168.2.4	0x20a4	No error (0)	www.youtub e.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	110005224.collect.igodigital.com	nova.collect.igodigital.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova.collect.igodigital.com	nova-collector-1192479543.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		3.221.235.248	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.5.138.229	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.72.141.113	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		18.204.189.7	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		18.214.4.88	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.73.82.215	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		54.208.116.125	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.303092957 CET	8.8.8.8	192.168.2.4	0x894e	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.205.84.122	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.320852995 CET	8.8.8.8	192.168.2.4	0x3821	No error (0)	cdn.levelaccess.net	cdn-backend.levelaccess.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:15.320852995 CET	8.8.8.8	192.168.2.4	0x3821	No error (0)	cdn-backend.levelaccess.net		13.224.94.91	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.320852995 CET	8.8.8.8	192.168.2.4	0x3821	No error (0)	cdn-backend.levelaccess.net		13.224.94.128	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.320852995 CET	8.8.8.8	192.168.2.4	0x3821	No error (0)	cdn-backend.levelaccess.net		13.224.94.35	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.320852995 CET	8.8.8.8	192.168.2.4	0x3821	No error (0)	cdn-backend.levelaccess.net		13.224.94.108	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.743423939 CET	8.8.8.8	192.168.2.4	0x3965	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:15.743423939 CET	8.8.8.8	192.168.2.4	0x3965	No error (0)	stats.l.doubleclick.net		74.125.71.154	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.743423939 CET	8.8.8.8	192.168.2.4	0x3965	No error (0)	stats.l.doubleclick.net		74.125.71.155	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.743423939 CET	8.8.8.8	192.168.2.4	0x3965	No error (0)	stats.l.doubleclick.net		74.125.71.157	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:15.743423939 CET	8.8.8.8	192.168.2.4	0x3965	No error (0)	stats.l.doubleclick.net		74.125.71.156	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova.collect.igodigital.com	nova-collector-1192479543.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		3.213.223.157	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		34.234.28.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		18.214.4.88	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		54.197.190.85	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.72.141.113	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		54.208.116.125	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.205.84.122	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.324203968 CET	8.8.8.8	192.168.2.4	0x322f	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.23.58.111	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:16.689728022 CET	8.8.8.8	192.168.2.4	0x6ab7	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.021692038 CET	8.8.8.8	192.168.2.4	0x75e3	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.021692038 CET	8.8.8.8	192.168.2.4	0x75e3	No error (0)	photos-ugc.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.047071934 CET	8.8.8.8	192.168.2.4	0x3e69	No error (0)	i.ytimg.com		142.250.180.150	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.147756100 CET	8.8.8.8	192.168.2.4	0x282d	No error (0)	syndication.twitter.com		104.244.42.136	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.147756100 CET	8.8.8.8	192.168.2.4	0x282d	No error (0)	syndication.twitter.com		104.244.42.72	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.147756100 CET	8.8.8.8	192.168.2.4	0x282d	No error (0)	syndication.twitter.com		104.244.42.200	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.147756100 CET	8.8.8.8	192.168.2.4	0x282d	No error (0)	syndication.twitter.com		104.244.42.8	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.293138027 CET	8.8.8.8	192.168.2.4	0xc772	No error (0)	cdn.syndication.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.293138027 CET	8.8.8.8	192.168.2.4	0xc772	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.293138027 CET	8.8.8.8	192.168.2.4	0xc772	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.293138027 CET	8.8.8.8	192.168.2.4	0xc772	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.819222927 CET	8.8.8.8	192.168.2.4	0xb375	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.819222927 CET	8.8.8.8	192.168.2.4	0xb375	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.819222927 CET	8.8.8.8	192.168.2.4	0xb375	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.819222927 CET	8.8.8.8	192.168.2.4	0xb375	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:17.886591911 CET	8.8.8.8	192.168.2.4	0xcad3	No error (0)	ton.twimg.com	cs511.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:17.886591911 CET	8.8.8.8	192.168.2.4	0xcad3	No error (0)	cs511.wpc.edgecastcdn.net		152.199.21.140	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:08:18.256746054 CET	8.8.8.8	192.168.2.4	0x99dd	No error (0)	zna8zta7cuf00ejmf-miamidadecounty.siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:18.256746054 CET	8.8.8.8	192.168.2.4	0x99dd	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:18.524050951 CET	8.8.8.8	192.168.2.4	0x9156	No error (0)	siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:18.524050951 CET	8.8.8.8	192.168.2.4	0x9156	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova.collect.igodigital.com	nova-collector-1192479543.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.23.58.111	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		3.221.235.248	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		34.234.28.0	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		3.213.223.157	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		18.214.4.88	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		54.162.220.59	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.72.141.113	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:19.820056915 CET	8.8.8.8	192.168.2.4	0x80a2	No error (0)	nova-collector-1192479543.us-east-1.elb.amazonaws.com		52.20.122.246	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:35.667639971 CET	8.8.8.8	192.168.2.4	0xfa89	No error (0)	sni1gl.wpc.gammacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:36.185945988 CET	8.8.8.8	192.168.2.4	0xef3b	No error (0)	api.levelaccess.net	api-backend.levelaccess.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:36.185945988 CET	8.8.8.8	192.168.2.4	0xef3b	No error (0)	api-backend.levelaccess.net	la-pr-analy-1p2sxho81cjid-1195857617.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:36.185945988 CET	8.8.8.8	192.168.2.4	0xef3b	No error (0)	la-pr-analy-1p2sxho81cjid-1195857617.us-east-1.elb.amazonaws.com		52.0.123.75	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:36.185945988 CET	8.8.8.8	192.168.2.4	0xef3b	No error (0)	la-pr-analy-1p2sxho81cjid-1195857617.us-east-1.elb.amazonaws.com		52.4.252.180	A (IP address)	IN (0x0001)
Feb 25, 2021 21:08:51.713155985 CET	8.8.8.8	192.168.2.4	0xf8ef	No error (0)	dc.services.visualstudio.com	dc.applicationinsights.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:51.713155985 CET	8.8.8.8	192.168.2.4	0xf8ef	No error (0)	dc.applicationinsights.azure.com	global.in.ai.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:08:51.713155985 CET	8.8.8.8	192.168.2.4	0xf8ef	No error (0)	global.in.ai.monitor.azure.com	global.in.ai.privatelink.monitor.azure.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:08:51.713155985 CET	8.8.8.8	192.168.2.4	0xf8ef	No error (0)	global.in.ai.privatelink.monitor.azure.com	dc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:07:40.673881054 CET	207.241.227.120	443	192.168.2.4	49726	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:17 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:07:40.677774906 CET	207.241.227.120	443	192.168.2.4	49727	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:17 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

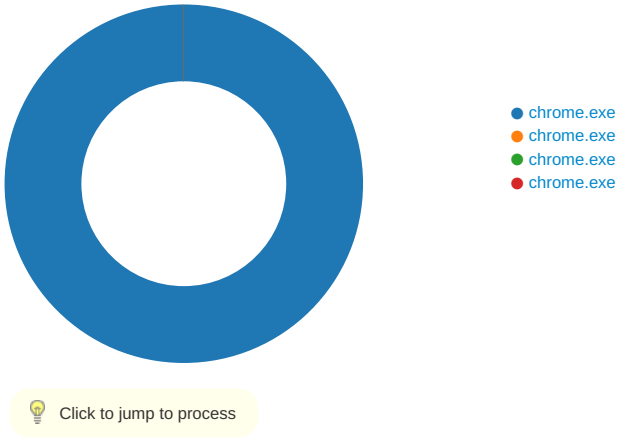
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:07:40.840358973 CET	207.241.227.120	443	192.168.2.4	49728	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019	Mon Feb 21 23:56:17 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 25, 2021 21:08:15.609131098 CET	3.221.235.248	443	192.168.2.4	49855	CN=*.collect.igodigital.com, O="SALESFORCE.COM, INC.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021	Sat Feb 26 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:08:16.679805040 CET	3.213.223.157	443	192.168.2.4	49858	CN=*.collect.igodigital.com, O="SALESFORCE.COM, INC.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021	Sat Feb 26 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:08:16.799031973 CET	3.213.223.157	443	192.168.2.4	49859	CN=*.collect.igodigital.com, O="SALESFORCE.COM, INC.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 25 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat Feb 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:08:17.266135931 CET	104.244.42.136	443	192.168.2.4	49866	CN=syndication.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 30 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Tue Nov 30 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Feb 25, 2021 21:08:36.443994045 CET	52.0.123.75	443	192.168.2.4	49946	CN=api.levelaccess.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 19 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 21 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6860 Parent PID: 1284

General

Start time:	21:07:36
Start date:	25/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://ia601400.us.archive.org/3/items/20210225_20210225_0759/accounts.miamidade.gov.html'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
						Source	

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 7124 Parent PID: 6860

General

Start time:	21:07:37
Start date:	25/02/2021
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 --field-trial-handle=1496,7194890310717246147,26815992129845608 3,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1736 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: chrome.exe PID: 6268 Parent PID: 6860

General

Start time:	21:08:18
Start date:	25/02/2021
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=audio.mojom.AudioService --field-trial-handle=1496,7194890310717246147,26815992129845608 3,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=3120 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 8164 Parent PID: 6860

General

Start time:	21:08:18
Start date:	25/02/2021
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=video_capture.mojom.VideoCaptureService --field-trial-handle=1496,7194890310717246147,268159921298456083,131072 --lang=en-GB --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=4288 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly