



ID: 404292
Cookbook: browseurl.jbs
Time: 21:46:08
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://www.casella.com/ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 12
Contacted IPs 13
Public 13
General Information 15
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 50
No static file info 50
Network Behavior 50
Network Port Distribution 50
TCP Packets 50
DNS Queries 52
DNS Answers 54
HTTP Request Dependency Graph 68
Code Manipulations 68
Statistics 69
Behavior 69
System Behavior 69
Analysis Process: iexplore.exe PID: 5488 Parent PID: 800 69
General 69
File Activities 69
Registry Activities 69
Analysis Process: iexplore.exe PID: 5840 Parent PID: 5488 70

Copyright Joe Security LLC 2021

General 70
File Activities 70
Registry Activities 70
Disassembly 70

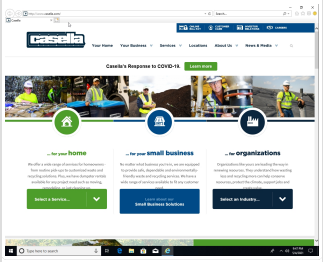
Analysis Report http://www.casella.com/

Overview

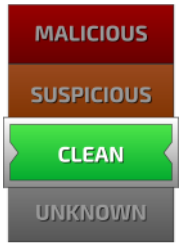
General Information

Sample URL:	http://www.casella.com/
Analysis ID:	404292
Infos:	

Most interesting Screenshot:



Detection



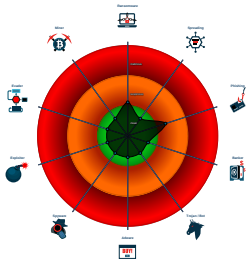
Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

HTML body contains low number of ...

HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5488 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5840 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5488 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

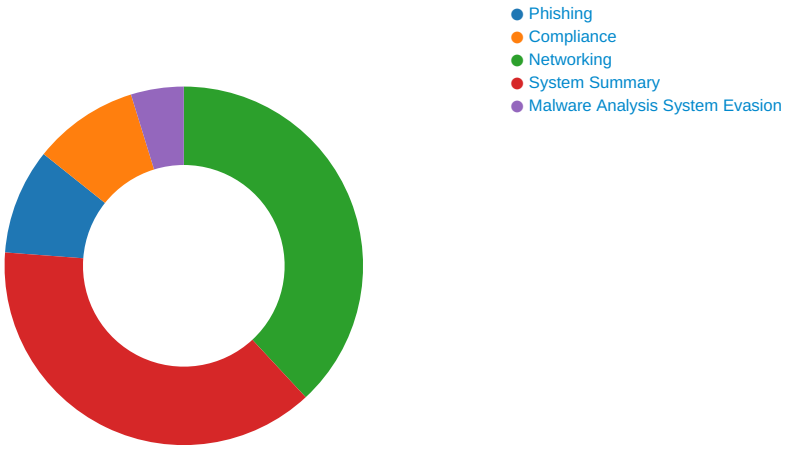
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



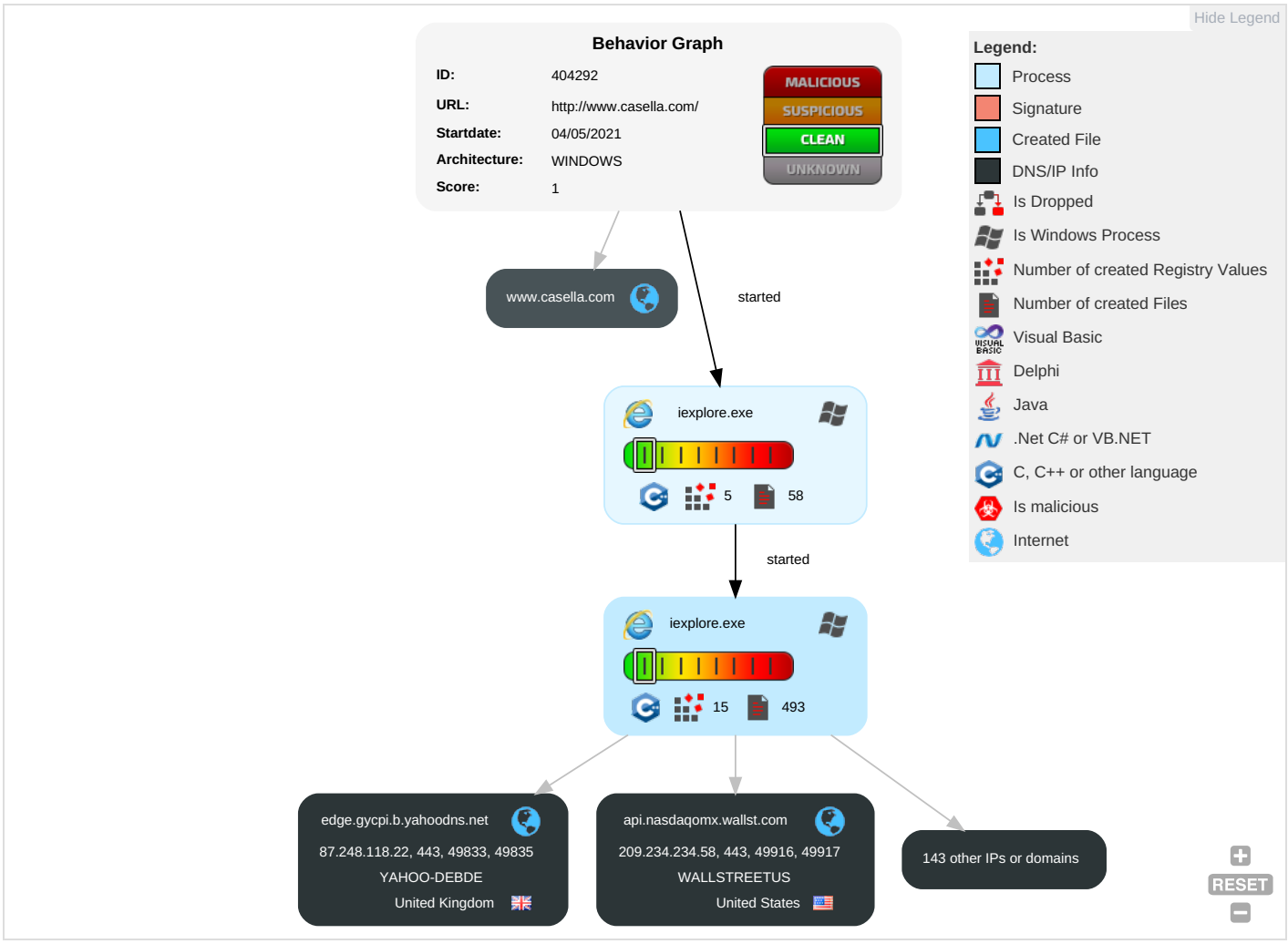
Click to jump to signature section

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

Mitre Att&ck Matrix

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

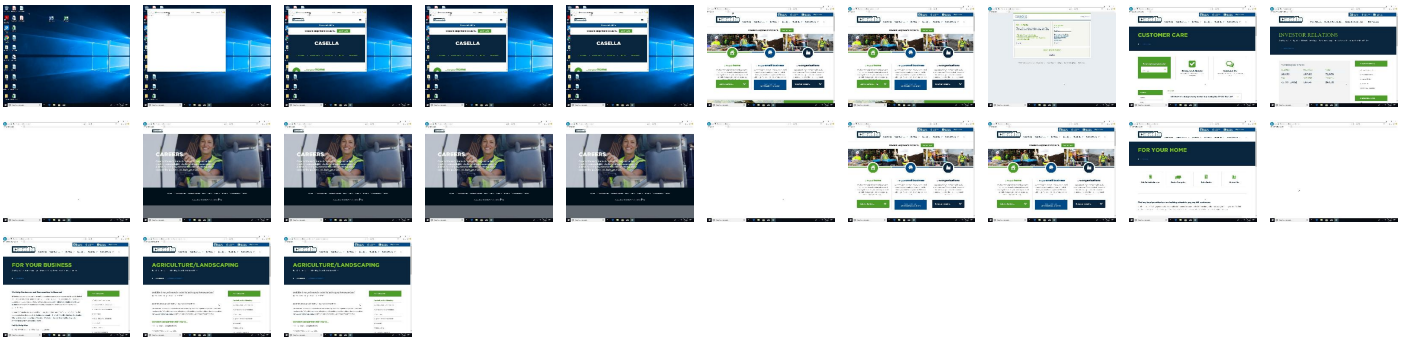
Behavior Graph

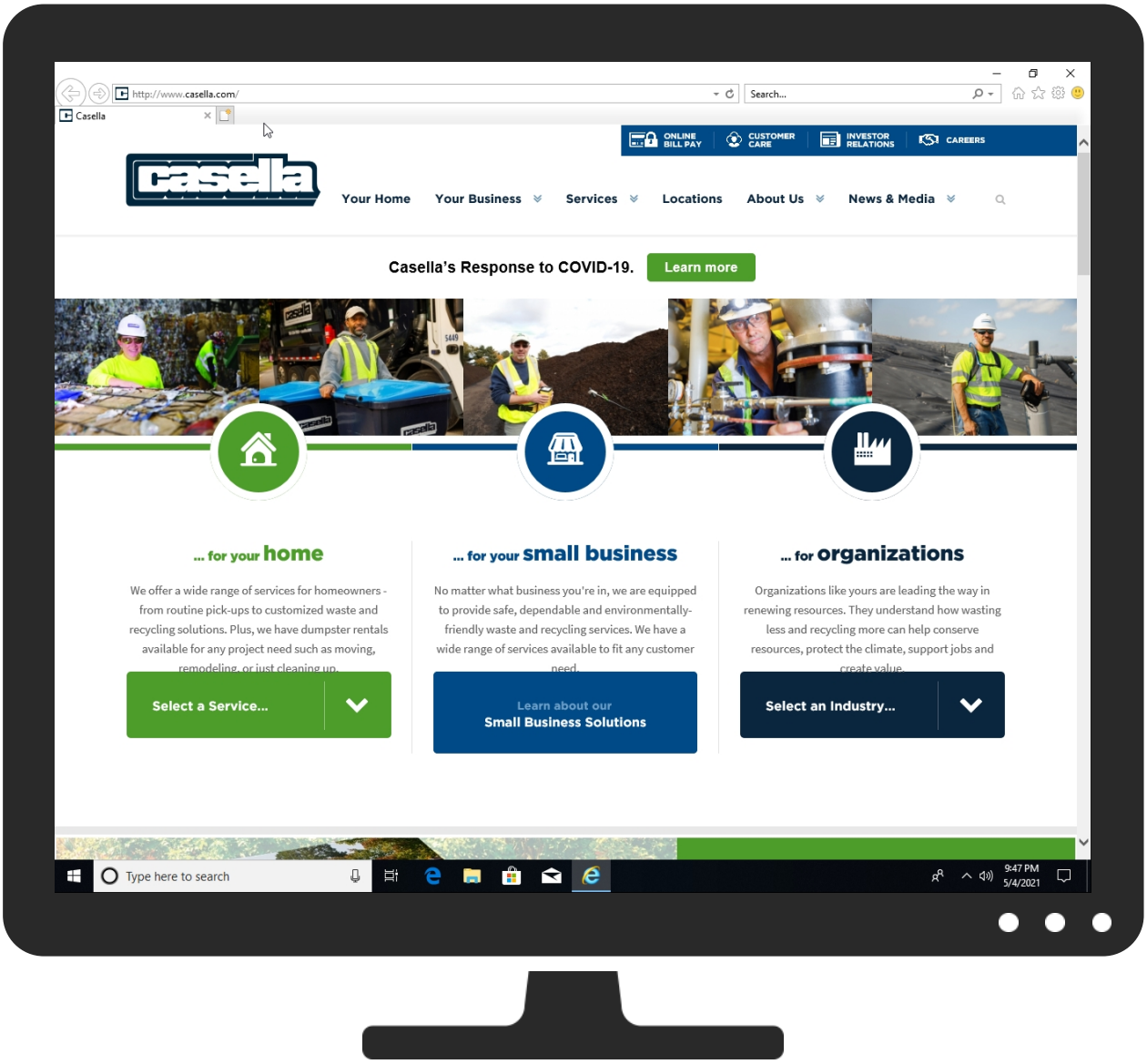


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.casella.com/	3%	Virustotal		Browse
http://www.casella.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
nydc1.outbrain.org	0%	Virustotal		Browse
bam.nr-data.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ir.casella.com/LOverview	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.casella.com/core/themes/stable/css/system/components/details.module.css?qpcosx	0%	Avira URL Cloud	safe	
http://https://www.casella.com/services/recycling/recycle-better?tab=Download_Free_Posters#tabs	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/i/favicons/favicon-32x32.png-	0%	Avira URL Cloud	safe	
http://www.casella.com/core/misc/favicon.ico	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/css/custom/home.css?qpcosx	0%	Avira URL Cloud	safe	
http://rtsys.rtrk.com.au/w3c/proxy_privacy_policy.html?path=/w3c	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/2016-11/fullWidthPromo2.jpg	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/1400x630/public/2016-12/Trailer%20dump_1.jpg?h=fab5421a&itok=NQMCUGPF	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/fonts/Gotham-Black.eot?	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/480x384/public/2016-11/BANNER-CurbsidePickup-1900x960.jpg?h=7a8a8cdf&itok=9P7rGhj3	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/css/custom/developer-overrides.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/plugins/sticky-kit/jquery.sticky-kit.js?v=1.x	0%	Avira URL Cloud	safe	
http://www.casella.com/core/themes/stable/css/system/components/ajax-progress.module.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/i/misc/customerCare-icon.png	0%	Avira URL Cloud	safe	
http://www.casella.com/siteproblem.asp	0%	Avira URL Cloud	safe	
http://www.casella.com/core/assets/vendor/picturefill/picturefill.min.js?v=3.0.3	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://www.casella.com/services/casella-sustainability	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/PHOTO-LisaM.jpg?h=2992ba0a&itok=WlhPwy-4	0%	Avira URL Cloud	safe	
http://www.casella.com/core/assets/vendor/matchMedia/matchMedia.min.js?v=0.2.0	0%	Avira URL Cloud	safe	
http://www.casella.com/P	0%	Avira URL Cloud	safe	
http://https://ir.casella.com/press-releases	0%	Avira URL Cloud	safe	
http://www.casella.com/core/themes/stable/css/system/components/item-list.module.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/css/custom/internal.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/768x614/public/2017-02/BANNER-Rolloff-2-1900x960.jpg?h=7a8a8cdf&itok=Qy_47eA6	0%	Avira URL Cloud	safe	
http://www.casella.com/core/themes/stable/css/system/components/fieldgroup.module.css?qpcosx	0%	Avira URL Cloud	safe	
http://ws.pusherapp.com/app/7686f91ffa51daedac98?protocol=7&client=js&version=2.2.4&flash=false	0%	Avira URL Cloud	safe	
http://www.casella.com/Root	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/css/lib/casella-master.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/(	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/480x216/public/2016-12/Trailer%20dump_1.jpg?h=fab5421a&itok=qmuYXibG	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/plugins/royalslider/skins/preloaders/preloader-white.gif	0%	Avira URL Cloud	safe	
http://www.casella.com/modules/contrib/paragraphs/css/paragraphs.unpublished.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/css/custom/adw-menu.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/core/themes/stable/css/system/components/position-container.module.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/plugins/royalslider/skins/universal/rs-universal.png	0%	Avira URL Cloud	safe	
http://www.casella.com/core/themes/stable/css/system/components/align.module.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/plugins/font-awesome-v.4.6.3/css/font-awesome.min.css?qpcosx	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/i/misc/career-icon2.png	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/480x384/public/2021-01/BANNER-SustainabilityReport20-1900x960.jpg?h=7a8a8cdf&itok=X4pFSupk	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/i/patterns/blueTrans.png	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/js/custom/faq.js?v=1.x	0%	Avira URL Cloud	safe	
http://https://ir.casella.com/corporate-governance/contact-the-board	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/1x1/public/2021-04/Screen%20Shot%202020-09-23%20at%2011.40.28%20AM.png?itok=qIqm1XJh	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/960x768/public/2016-11/BANNER-CurbsidePickup-1900x960.jpg?h=7a8a8cdf&itok=Q1KFV8e9	0%	Avira URL Cloud	safe	
http://www.casella.com/sites/default/files/styles/480x384/public/2018-03/BANNER-RecycleRight-1900x960.jpg?h=7a8a8cdf&itok=OVikH09Q	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/js/custom/google_analytics_event_tracking.js?v=1.x	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/i/misc/payBill-icon.png	0%	Avira URL Cloud	safe	
http://www.casella.com/themes/custom/casella/js/custom/home.min.js?v=1.x	0%	Avira URL Cloud	safe	
http://https://ir.casella.com/environment	0%	Avira URL Cloud	safe	
http://www.casella.com/form/318	0%	Avira URL Cloud	safe	
http://www.casella.com/your-businessj	0%	Avira URL Cloud	safe	
http://https://www.casella.com/available-careers	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scontent-frx5-1.xx.fbcdn.net	185.60.216.19	true	false		high
eu-u.openx.net	34.98.64.218	true	false		high
mt1-ws-1895636413.us-east-1.elb.amazonaws.com	3.208.175.180	true	false		high
dyrxq3369g3sr.cloudfront.net	65.9.66.12	true	false		high
scontent-mia3-2.xx.fbcdn.net	157.240.14.19	true	false		high
adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com	54.78.31.47	true	false		high
elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com	3.123.96.39	true	false		high
61870c77-2e72-45dc-9f17-2f74952d866e.rlets.com	52.88.192.45	true	false		unknown
ih.adscale.de	18.197.81.144	true	false		high
mwzeom.zeotap.com	172.67.13.182	true	false		high
sync.crwdcntrl.net	54.194.226.253	true	false		high
cm.g.doubleclick.net	142.250.185.162	true	false		high
idaas-ext.cph.liveintent.com	54.81.208.30	true	false		high
rtb-csync-itx4.smartadserver.com	185.86.139.89	true	false		high
scontent-iad3-1.xx.fbcdn.net	31.13.66.19	true	false		high
idaas6.cph.liveintent.com	3.209.93.152	true	false		high
eu2-ice.360yield.com	52.58.206.142	true	false		high
nydc1.outbrain.org	64.202.112.127	true	false	• 0%, Virustotal, Browse	unknown
us-u.openx.net	35.244.159.8	true	false		high
stats.l.doubleclick.net	74.125.133.154	true	false		high
secure3.i-doxs.net	209.112.4.23	true	false		high
uip.semasio.net	77.243.60.138	true	false		high
ad.sxp.smartclip.net	34.252.166.236	true	false		high
bam.nr-data.net	162.247.242.18	true	false	• 0%, Virustotal, Browse	unknown
d3bi9sbave64gz.cloudfront.net	65.9.66.129	true	false		high
googleads.g.doubleclick.net	216.58.212.162	true	false		high
ams01.sync.search.spotxchange.com	185.94.180.125	true	false		high
ams-1-sync.go.sonobi.com	178.162.133.149	true	false		high
capture-api.reachlocalservices.com	99.86.2.69	true	false		unknown
envoy-public.liqadprdct-capture-production-us-east1.gke-eric-eyre-svc.gannettdigital.com	34.75.237.118	true	false		high
awseb-awseb-eghbt6mzdw45-44179265.us-east-1.elb.amazonaws.com	52.0.228.129	true	false		high
prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com	34.246.207.243	true	false		high
adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	52.215.226.121	true	false		high
aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	35.176.232.241	true	false		high
pixel-origin.mathtag.com	185.29.133.52	true	false		high
alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com	18.195.73.36	true	false		high
dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com	3.228.139.221	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	18.200.157.96	true	false		high
scontent-bos3-1.xx.fbcdn.net	157.240.220.14	true	false		high
ec2-18-233-7-102.compute-1.amazonaws.com	18.233.7.102	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
i.simpli.fi	169.50.137.179	true	false		high
scontent-ort2-2.xx.fbcdn.net	157.240.18.19	true	false		high
scontent-iad3-2.xx.fbcdn.net	157.240.229.1	true	false		high
am-vip001.taboola.com	141.226.228.48	true	false		high
www.google.de	142.250.185.227	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
tag.simpli.fi	169.50.137.179	true	false		high
star.c10r.facebook.com	31.13.92.10	true	false		high
scontent-dfw5-1.xx.fbcdn.net	157.240.19.26	true	false		high

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ssp.ads.betweendigital.com	96.46.186.57	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	52.57.10.248	true	false		unknown
tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	52.28.108.245	true	false		high
match-243508202.us-west-2.elb.amazonaws.com	44.241.59.199	true	false		high
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
api.nasdaqomx.wallst.com	209.234.234.58	true	false		high
www.casella.com	52.87.65.167	true	false		unknown
ib.anycast.adnxs.com	185.33.221.15	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	18.156.0.31	true	false		unknown
naw.vap.lijit.com	63.251.14.14	true	false		high
load-euw1.exelator.com	54.78.254.47	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		unknown
apps.twinesocial.com	unknown	unknown	false		high
a.adroll.com	unknown	unknown	false		high
d.adroll.com	unknown	unknown	false		high
stats.pusher.com	unknown	unknown	false		high
id5-sync.com	unknown	unknown	false		unknown
sync.go.sonobi.com	unknown	unknown	false		high
ads.stickyadstv.com	unknown	unknown	false		unknown
cm.everesttech.net	unknown	unknown	false		high
cdn.rlets.com	unknown	unknown	false		unknown
thenasdaqomxgroup.demdex.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
ir.casella.com	unknown	unknown	false		unknown
token.rubiconproject.com	unknown	unknown	false		high
ice.360yield.com	unknown	unknown	false		high
match.adsrvr.org	unknown	unknown	false		high
i6.liadm.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
ce.lijit.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
simage2.pubmatic.com	unknown	unknown	false		high
apps-cdn.twinesocial.com	unknown	unknown	false		high
uipglob.semasio.net	unknown	unknown	false		high
c-11158-20201221-www-casella-com.i.icims.com	unknown	unknown	false		high
stags.bluekai.com	unknown	unknown	false		high
sync.mathtag.com	unknown	unknown	false		high
careers-casella.icims.com	unknown	unknown	false		high
pixel.mathtag.com	unknown	unknown	false		high
d.adroll.mgr.consensu.org	unknown	unknown	false		unknown
s.go-mpulse.net	unknown	unknown	false		unknown
ups.analytics.yahoo.com	unknown	unknown	false		high
ws.pusherapp.com	unknown	unknown	false		unknown
external-iad3-1.xx.fbcdn.net	unknown	unknown	false		high
d.agkn.com	unknown	unknown	false		high
ads.yahoo.com	unknown	unknown	false		high
rtb-csync.smartadserver.com	unknown	unknown	false		high
ads.betweendigital.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.casella.com/your-business/agriculturelandscaping	false		unknown
http://www.casella.com/core/themes/stable/css/system/components/details.module.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/core/misc/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://apps-cdn.twinesocial.com/images/emoji/66.svg	false		high
http://www.casella.com/themes/custom/casella/css/custom/home.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/sites/default/files/2016-11/fullWidthPromo2.jpg	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/sites/default/files/styles/1400x630/public/2016-12/Trailer%20dump_1.jpg?h=fab5421a&itok=NQMCUGPF	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/fonts/Gotham-Black.eot?	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.casella.com/sites/default/files/styles/480x384/public/2016-11/BANNER-CurbsidePickup-1900x960.jpg?h=7a8a8cdf&itok=9P7rGhj3	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/css/custom/developer-overrides.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/plugins/sticky-kit/jquery.sticky-kit.js?v=1.x	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/core/themes/stable/css/system/components/ajax-progress.module.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/your-business/agriculturelandscaping	false		unknown
http://www.casella.com/themes/custom/casella/i/misc/customerCare-icon.png	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/core/assets/vendor/picturefill/picturefill.min.js?v=3.0.3	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/your-business	false		unknown
http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/PHOTO-LisaM.jpg?h=2992ba0a&itok=WlhPwy-4	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/core/assets/vendor/matchMedia/matchMedia.min.js?v=0.2.0	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/your-business	false		unknown
http://www.casella.com/core/themes/stable/css/system/components/item-list.module.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/css/custom/internal.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://apps.twinesocial.com/css/player/embed.css	false		high
http://apps-cdn.twinesocial.com/css/webfonts/fa-brands-400.eot?	false		high
http://www.casella.com/sites/default/files/styles/768x614/public/2017-02/BANNER-Rolloff-2-1900x960.jpg?h=7a8a8cdf&itok=Qy_47eA6	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/core/themes/stable/css/system/components/fieldgroup.module.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://ws.pusherapp.com/app/7686f91ffa51daedac98?protocol=7&client=js&version=2.2.4&flash=false	false	• Avira URL Cloud: safe	unknown
http://apps-cdn.twinesocial.com/css-min/files/player%252Ftheme-font%252Fopen-sans+player%252Fselect2.css+player%252Fselect2-bootstrap.css+player%252Ftw-fonts.css+player%252Fbootstrap-3.1.1.min.css+player%252Ffont-awesome.min.css+player%252Ftheme-layout%252Fbase.css+player%252Fembed.css+player%252Ftheme-modal%252Fbase.css+player%252Ftheme-layout%252Fclassic+player%252Ftheme-color%252Fwhite/v/2.21/t/1612366471.css	false		high
http://www.casella.com/themes/custom/casella/css/lib/casella-master.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/sites/default/files/styles/480x216/public/2016-12/Trailer%20dump_1.jpg?h=fab5421a&itok=qmuYXibG	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/plugins/royalslider/skins/preloaders/preloader-white.gif	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/modules/contrib/paragraphs/css/paragraphs.unpublished.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/	false		unknown
http://www.casella.com/themes/custom/casella/css/custom/adw-menu.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://apps-cdn.twinesocial.com/css/webfonts/fa-light-300.eot?	false		high
http://www.casella.com/core/themes/stable/css/system/components/position-container.module.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/plugins/royalslider/skins/universal/rs-universal.png	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/core/themes/stable/css/system/components/align.module.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/plugins/font-awesome-v.4.6.3/css/font-awesome.min.css?qpcosx	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/i/misc/career-icon2.png	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/sites/default/files/styles/480x384/public/2021-01/BANNER-SustainabilityReport20-1900x960.jpg?h=7a8a8cdf&itok=X4pFSupk	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/i/patterns/blueTrans.png	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/js/custom/faq.js?v=1.x	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/	false		unknown
http://www.casella.com/sites/default/files/styles/1x1/public/2021-04/Screen%20Shot%202020-09-23%20at%2011.40.28%20AM.png?itok=qIqm1XJh	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/sites/default/files/styles/960x768/public/2016-11/BANNER-CurbsidePickup-1900x960.jpg?h=7a8a8cdf&itok=Q1KFV8e9	false	• Avira URL Cloud: safe	unknown
http://https://secure3.i-doxs.net/casella/default.asp	false		high
http://www.casella.com/sites/default/files/styles/480x384/public/2018-03/BANNER-RecycleRight-1900x960.jpg?h=7a8a8cdf&itok=OVikH09Q	false	• Avira URL Cloud: safe	unknown
http://apps-cdn.twinesocial.com/images/emoji/111.svg	false		high
http://www.casella.com/themes/custom/casella/js/custom/google_analytics_event_tracking.js?v=1.x	false	• Avira URL Cloud: safe	unknown

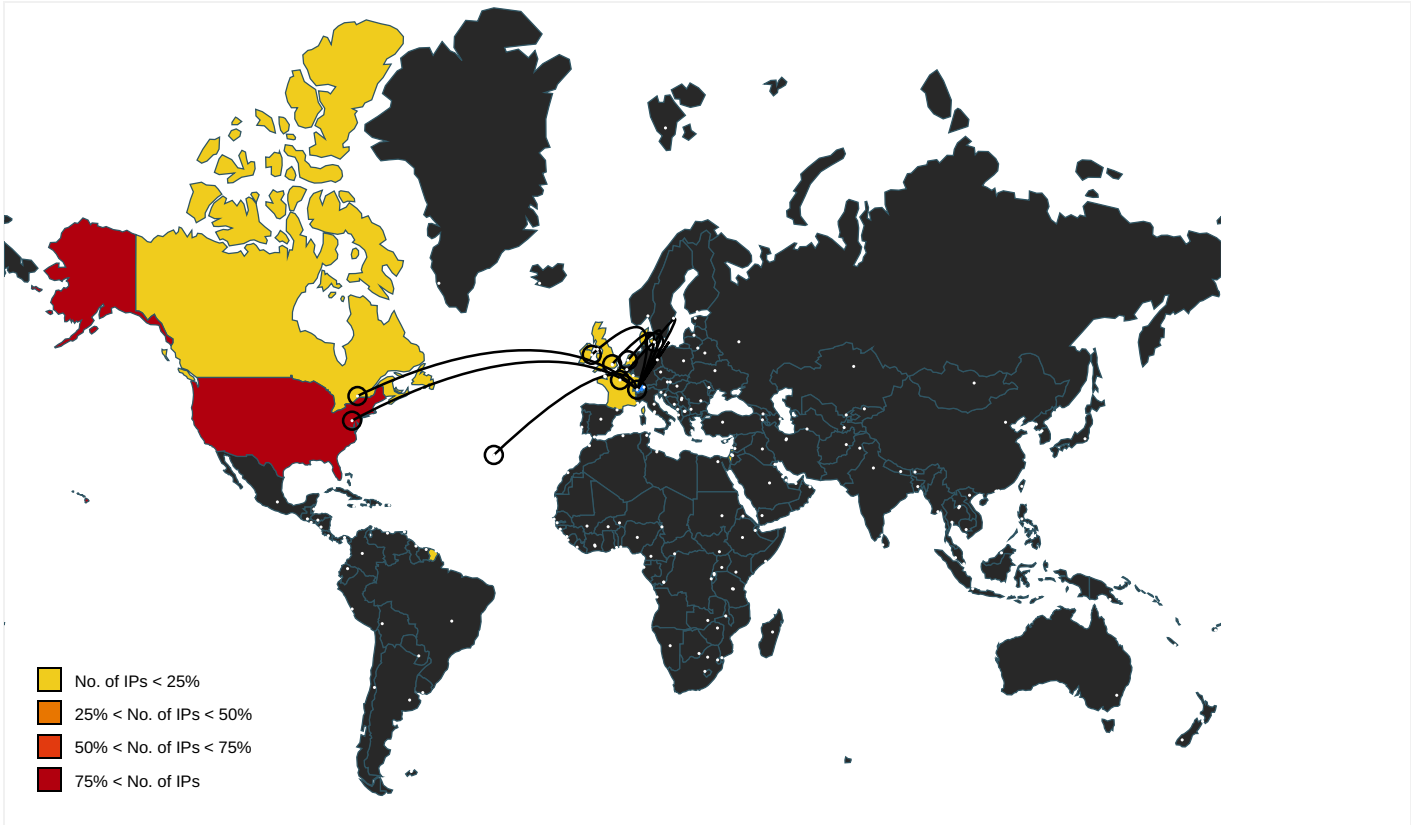
Name	Malicious	Antivirus Detection	Reputation
http://stats.pusher.com/timeline/v2/jsonp/1?session=ODQwNTk1ODM3&bundle=MQ%3D%3D&key=NzY4NmY5MWZmYTUxZGFlZGFjOTg%3D&lib=anM%3D&version=Mi4yLjQ%3D&features=WyJ3cyIsImZsYXNoIl0%3D&timeline=W3siaW5zdGFuY2VzIjoxLCJ0aW1lc3RhbXAiOjE2MjAxNTc2NzM5OTd9LHsic3RhdGUiOiJjb25uZWN0aW5nIiwidGltZXN0YW1wIjoxNjIwMTU3NjczOTk3fSx7ImNhY2hlZCI6dHJ1ZSwidHJhbnNwb3J0Ijoid3MiLCJsYXRlbmN5IjoxNzE0LCJ0aW1lc3RhbXAiOjE2MjAxNTc2NzM5OTd9LHsiY2lkIjoxLCJ0cmFuc3BvcnQiOiJ3cyIsInRpbWVzdGFtcCI6MTYyMDE1NzY3NTk2OH0seyJaWQiOjEsInN0YXRlIjoiaW5pdGlhbGl6ZWQiLCJ0aW1lc3RhbXAiOjE2MjAxNTc2NzM5OTh9LHsiY2lkIjoxLCJzdGF0ZSI6ImNvbm5lY3RpbmciLCJ0aW1lc3RhbXAiOjE2MjAxNTc2NzM5OTh9LHsiY2lkIjoxLCJzdGF0ZSI6Im9wZW4iLCJ0aW1lc3RhbXAiOjE2MjAxNTc2NzQ3OTJ9LHsic3RhdGUiOiJjb25uZWN0ZWQiLCJwYXJhbXMiOnsic29ja2V0X2lkIjoiMzE2Mjk3LjI0Nzc5Mzg5In0sInRpbWVzdGFtcCI6MTYyMDE1NzY3NDkzOH1d	false		high
http://https://ir.casella.com/	false		unknown
http://www.casella.com/themes/custom/casella/i/misc/payBill-icon.png	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/js/custom/home.min.js?v=1.x	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/your-business/chains-multi-site-retailers	false		unknown
http://www.casella.com/#menu	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ir.casella.com/LOverview	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ogp.me/ns#	LPC26D7B.htm.3.dr	false		high
http://https://www.casella.com/services/recycling/recycle-better?tab=Download_Free_Posters#tabs	55F3ZRAZ.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/themes/custom/casella/i/favicons/favicon-32x32.png-	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://casellawastesystems.gcs-web.com/	LPC26D7B.htm.3.dr	false		high
http://https://connect.facebook.net/en_US/all.js#xfbml=1&status=1&version=v2.5	casella[1].htm.3.dr	false		high
http://https://careers-casella.icims.com/s/g/files/knoqqb53536/files/favicon-32x32.png	~DF6CBADDF41D1DC3B0.TMP.1.dr	false		high
http://rtsys.rtrk.com.au/w3c/proxy_privacy_policy.html?path=/w3c	e7245dc9f172f74952d866e[1].js0.3.dr	false	• Avira URL Cloud: safe	unknown
http://js.pusher.com/	pusher.min[1].js.3.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	fa-solid-900[1].eot.3.dr, fa-regular-400[1].eot.3.dr, fa-light-300[1].eot.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.adroll.com	roundtrip[1].js.3.dr, agriculturelandscaping[1].htm.3.dr	false		high
http://www.casella.com/#menu	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		unknown
http://https://fontawesome.com	fa-solid-900[1].eot.3.dr, 1612366471[1].css.3.dr	false		high
http://https://github.com/scottjehl/picturefill/blob/master/Authors.txt;	picturefill.min[1].js0.3.dr	false		high
http://www.casella.com/siteproblem.asp	default[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/MoonScript/jQuery-ajaxTransport-XDomainRequest	embed[1].js.3.dr	false		high
http://getbootstrap.com)	1612366471[1].css.3.dr	false	• Avira URL Cloud: safe	low
http://https://www.casella.com/services/casella-sustainability	LPC26D7B.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/company/casella-waste-systems	agriculturelandscaping[1].htm.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://www.casella.com/P	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.twinesocial.com/images/favicon/favicon-16x16.png	casella[1].htm.3.dr	false		high
http://www.typography.com/support/eula.html	Gotham-Bold[1].eot.3.dr	false		high
http://https://ir.casella.com/press-releases	agriculturelandscaping[1].htm.3.dr, LPC26D7B.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://rtsys.rtrk.com/w3c/proxy_privacy_policy.html?path=/w3c	e7245dc9f172f74952d866e[1].js0.3.dr	false		high
http://https://static.twinesocial.com/images/favicon/apple-touch-icon.png	casella[1].htm.3.dr	false		high
http://https://careers-casella.icims.com/	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr, agriculturelandscaping[1].htm.3.dr, 55F3ZRAZ.htm.3.dr, ~DF6CBADDF41D1DC3B0.TMP.1.dr	false		high
http://https://secure3.i-doxs.net/casella/default.asp	LPC26D7B.htm.3.dr	false		high
http://www.casella.com/Root	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://feeds.feedburner.com/casella/MwAD	LPC26D7B.htm.3.dr	false		high
http://www.casella.com/(	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.typography.com/support/eula.html.A	Gotham-Bold[1].eot.3.dr, Gotham-Black[1].eot0.3.dr	false		high
http://https://www.youtube.com/c/CasellaWasteSystems	agriculturelandscaping[1].htm.3.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	1612366471[1].css.3.dr	false		high
http://https://ir.casella.com/corporate-governance/contact-the-board	LPC26D7B.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://tag.simpli.fi/sifitag/da06ef10-8b00-0137-57d2-06659b33d47c	agriculturelandscaping[1].htm.3.dr	false		high
http://https://www.instagram.com/casellawaste/	agriculturelandscaping[1].htm.3.dr	false		high
http://https://ir.casella.com/environment	LPC26D7B.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.casella.com/#main-content	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF6CBADDF41D1DC3B0.TMP.1.dr	false		unknown
http://https://www.linkedin.com/company/casella-waste-systems	LPC26D7B.htm.3.dr	false		high
http://www.casella.com/form/318	default[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.nasdaqomx.wallst.com/api/chart?display=mountain&symbol=CWST.OQ-cwst&scale=linear&duratio	LPC26D7B.htm.3.dr	false		high
http://www.casella.com/your-businessj	~DF6CBADDF41D1DC3B0.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ir.casella.com/	{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		unknown
http://https://www.casella.com/available-careers	LPC26D7B.htm.3.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.246.207.243	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
172.67.13.182	mwzeom.zeotap.com	United States		13335	CLOUDFLARENETUS	false
54.78.31.47	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
18.197.81.144	ih.adscale.de	United States		16509	AMAZON-02US	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.240.220.14	scontent-bos3-1.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
3.208.175.180	mt1-ws-1895636413.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
185.33.221.15	ib.anycast.adnxs.com	Netherlands		29990	ASN-APPNEXUS	false
99.86.2.69	capture-api.reachlocalservices.com	United States		16509	AMAZON-02US	false
77.243.60.138	uip.semasio.net	Denmark		42697	NETIC-ASDK	false
169.50.137.179	i.simpli.fi	United States		36351	SOFTLAYERUS	false
34.75.237.118	envoy-public.liqadprdct-capture-production-us-east1.gke-eric-eyre-svc.gannettdigital.com	United States		15169	GOOGLEUS	false
52.0.228.129	awseb-awseb-eghbt6mzdw45-44179265.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
52.88.192.45	61870c77-2e72-45dc-9f17-2f74952d866e.rlets.com	United States		16509	AMAZON-02US	false
65.9.66.12	dyrxq3369g3sr.cloudfront.net	United States		16509	AMAZON-02US	false
35.227.248.159	pixel.tapad.com	United States		15169	GOOGLEUS	false
34.252.166.236	ad.sxp.smartclip.net	United States		16509	AMAZON-02US	false
52.58.206.142	eu2-ice.360yield.com	United States		16509	AMAZON-02US	false
31.13.66.19	scontent-iad3-1.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
35.176.232.241	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
63.251.14.14	naw.vap.lijit.com	United States		32475	SINGLEHOP-LLCUS	false
157.240.19.26	scontent-dfw5-1.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
185.86.139.89	rtb-csync-itx4.smartadserver.com	France		201081	SMARTADSERVERFR	false
18.195.73.36	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
178.162.133.149	ams-1-sync.go.sonobi.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
18.156.0.31	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
18.233.7.102	ec2-18-233-7-102.compute-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
157.240.18.19	scontent-ort2-2.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
216.58.212.162	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
35.244.174.68	idsync.rlcdn.com	United States		15169	GOOGLEUS	false
3.209.93.152	idaas6.cph.liveintent.com	United States		14618	AMAZON-AESUS	false
209.112.4.23	secure3.i-doxs.net	Canada		15290	ALLST-15290CA	false
185.29.133.52	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false
44.241.59.199	match-243508202.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
52.87.65.167	www.casella.com	United States		14618	AMAZON-AESUS	false
74.125.133.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
31.13.92.10	star.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
52.57.10.248	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
157.240.14.19	scontent-mia3-2.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
54.78.254.47	load-euw1.exelator.com	United States		16509	AMAZON-02US	false
35.244.159.8	us-u.openx.net	United States		15169	GOOGLEUS	false
3.123.96.39	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
185.94.180.125	ams01.sync.search.spotxchange.com	Netherlands		35220	SPOTX-AMSNL	false
96.46.186.57	ssp.ads.betweendigital.com	United States		7979	SERVERS-COMUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.28.108.245	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
185.64.189.110	pug22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
18.200.157.96	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.185.162	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
141.226.228.48	am-vip001.taboola.com	Israel		200478	TABOOLA-ASIL	false
65.9.66.129	d3bi9sbave64gz.cloudfront.net	United States		16509	AMAZON-02US	false
3.228.139.221	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
64.202.112.127	nydc1.outbrain.org	United States		22075	AS-OUTBRAINUS	false
51.89.7.199	unknown	France		16276	OVHFR	false
157.240.229.1	scontent-iad3-2.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
54.194.226.253	sync.crwdcntrl.net	United States		16509	AMAZON-02US	false
52.215.226.121	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
185.60.216.19	scontent-frx5-1.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
34.98.64.218	eu-u.openx.net	United States		15169	GOOGLEUS	false
54.81.208.30	idaas-ext.cph.liveintent.com	United States		14618	AMAZON-AESUS	false
162.247.242.18	bam.nr-data.net	United States		23467	NEWRELIC-AS-1US	false
209.234.234.58	api.nasdaqomx.wallst.com	United States		7334	WALLSTREETUS	false
52.210.171.182	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404292
Start date:	04.05.2021
Start time:	21:46:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.casella.com/
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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@3/364@88/63

Copyright Joe Security LLC 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: http://www.casella.com/#main-content • Browsing link: https://secure3.i-doxs.net/casella/default.asp • Browsing link: http://www.casella.com/faq • Browsing link: http://ir.casella.com/ • Browsing link: https://careers-casella.icims.com/ • Browsing link: http://www.casella.com/ • Browsing link: http://www.casella.com/#menu • Browsing link: http://www.casella.com/your-home • Browsing link: http://www.casella.com/your-business • Browsing link: http://www.casella.com/your-business/agriculturelandscaping • Browsing link: http://www.casella.com/your-business/chains-multi-site-retailers
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 184.87.213.153, 52.255.188.83, 23.5.103.140, 142.250.184.234, 184.87.212.223, 142.250.186.40, 172.217.16.130, 142.250.185.142, 142.250.185.227, 142.250.184.196, 142.250.186.170, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 2.20.143.32, 2.20.142.228, 173.222.105.15, 173.222.105.33, 142.250.185.67, 204.79.197.200, 13.107.21.200, 23.57.81.215, 69.173.144.139, 69.173.144.138, 69.173.144.165, 20.82.210.154, 95.100.252.216, 95.100.252.91, 23.57.80.54, 34.250.153.194, 34.255.166.243, 54.194.191.134, 54.171.42.33, 99.81.11.244, 34.253.145.149, 162.247.243.147, 162.247.243.146, 23.37.59.116, 152.199.19.161, 92.122.246.223, 23.211.4.169, 2.19.68.144, 184.87.213.138, 23.37.54.146, 92.122.213.194, 92.122.213.247, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 52.155.217.156, 20.54.26.129 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, tags.bluekai.com.edgekey.net, arc.msn.com.nsatc.net, uipglob.trafficmanager.net, tls12.newrelic.com.cdn.cloudflare.net, cn-assets.adobedtm.com.edgekey.net, leapfrog-ssl-15399.edgekey.net, e11290.dspg.akamaiedge.net, e9126.x.akamaiedge.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, www.google-analytics.com, ip46.go-mpulse.net.edgekey.net, fonts.googleapis.com, e15399.dsca.akamaiedge.net, e11676.b.akamaiedge.net, ajax.googleapis.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, cm.everesttech.net.akadns.net, 2-01-275d-002d.cdx.cedexis.net, e4016.a.akamaiedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, cidr1.ads.stickyadstv.com.akadns.net, ris.api.iris.microsoft.com, sadroll.edgekey.net, store-images.s-microsoft.com, wildcard.icims.com.edgekey.net, wildcard46.go-mpulse.net.edgekey.net, blobcollector.events.data.trafficmanager.net, dsum-sec.casalemedia.com.edgekey.net, e10784.a.akamaiedge.net, e83137.dscb.akamaiedge.net, cs9.wpc.v0cdn.net, h2.shared.global.fastly.net, www.googleadservices.com, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, pixel.mathtag.com.edgekey.net, a.adroll.com.edgesuite.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, e8037.g.akamaiedge.net, www.googletagmanager.com, stickyadstv.com.edgekey.net, bat.bing.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, e4518.dscx.akamaiedge.net, ip2.ads.stickyadstv.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net,

e6791.b.akamaiedge.net, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, f4.shared.global.fastly.net, sync.search-gtm.spotxchange.com.akadns.net, a1945.g.akamai.net, e4518.dscapi7.akamaiedge.net, ip1.ads.stickyadstv.com.akadns.net, skypedataprdcoleus17.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, e7808.dscg.akamaiedge.net, go.microsoft.com.edgekey.net, ds-m.addthisedge.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtReadFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

No simulations

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\Local\Microsoft\Internet Explorer\DOMStore\BACZYXTY\apps.twinesocial[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	410

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BACZYXTY\apps.twinesocial[1].xml	
Entropy (8bit):	5.008957183924771
Encrypted:	false
SSDEEP:	12:JsrUCDe8slrSAVO9u0rUCDe85LSAVO1dqDiq:WU/8slr7VO9usU/8p7VO1dqDiq
MD5:	2AB552E92FAEAB017C6DD8D0CC980B33
SHA1:	9ABBA126C33DBB878D172BB790FFD74D9C30BAF5
SHA-256:	CF531DB87B0C50361214A36027E39930245061D2CEA4308EA4B94F1BB2D63E3B
SHA-512:	1DD08359F33C9FAE5D28AAEBD6DD9C7B90CAC88271878D8640DB16ACB2C9B44C6C9CF6B0366492C86402E6C04515A77A05BBE4098DD5969F5E2B4FB80748F3B
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="pusherTransportUnencrypted" value="{"timestamp":1620157627733,"transport":"ws","latency":1714}" ltime="1142076704" htime="30884126" /></root><root><item name="pusherTransportUnencrypted" value="{"timestamp":1620157674925,"transport":"ws","latency":928}" ltime="1613836704" htime="30884126" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BC6XF3KU\ir.casella[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	135
Entropy (8bit):	4.73404550280935
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsnObemKmlULF0VqHlJR3vAmBRMIAqSf6lKoaKb:JFK1rUFjgemKm6GVqHlJR3omBqlcb
MD5:	63AC654DBBE798AE3A6D78805C13D17F
SHA1:	AFF977028538F01C0B6428935B70A395CCF52714
SHA-256:	A601882070EC29CF18E6C893B8042ED4F0C596C4D0016984A7D71F4AAB52A1B7
SHA-512:	E1A47212946EF4F91438652A1E680073D7FF8D8CB95034215327F57BDF1A5F3D7FC8DFFDD2F4E815D7E9538A13A7E425DC8F4A0DB2EDA5756BAD2F426C84092
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="1326926704" htime="30884126" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\careers-casella.icims[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	12162
Entropy (8bit):	5.010504890267369
Encrypted:	false
SSDEEP:	192:oDQclqDQclWDQclEW4DQclEWo96DQclEWo9mDQclEWo9mDQclEWo9DDQclEWo9Rz:CZUZQZEWSZEWo9kZEWo9gZEWo9gZEWoY
MD5:	423D1372EF37B933995EEE6451292AEC
SHA1:	42E098B9FBD645120BC6DC6AB43F16FE0D23FC3E
SHA-256:	4A24180E982683C51C690E781B32CCEBF1598F3671162AD379C368A4FBF56066
SHA-512:	0E95BFBE0FCC7E175E9687BAEDBF9D77D50D25AD9C5341FB11E22D649FCD86E5DE54ADDB4D65497E886E40EDFBECC014DEB13752EB291E6DB9FB4340C0575EC
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1350216704" htime="30884126" /></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1350216704" htime="30884126" /><item name="61870c77-2e72-45dc-9f17-2f74952d866e_override_site_id" value="" ltime="1360916704" htime="30884126" /></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1350216704" htime="30884126" /><item name="61870c77-2e72-45dc-9f17-2f74952d866e_override_site_id" value="" ltime="1360916704" htime="30884126" /></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1350216704" htime="30884126" /><item name="61870c77-2e72-45dc-9f17-2f74952d866e_override_site_id" value="" ltime="1360916704" htime="30884126" /><item name="rl_initial_referrer" value="" ltime="1368456704" htime="30884126" /><item name="rl_initial_page_uri" value="https://care

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.casella[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	93320
Entropy (8bit):	5.0013647929901195
Encrypted:	false
SSDEEP:	1536:zhh6X9XnX+XDXGXjXgXgXXXJXMTYThoThBThcThcThvTh5ThkJUJbJ2J2JiJl3Ti:V
MD5:	DB8EF61A342E6CE1D36BD99C1A3CCCB8
SHA1:	80A82E7493E16463E3F2A581006B5314ED50A1F2
SHA-256:	12AC1C5073585032DF8A9099F2333162328C996B00CD2FC6A2348856FB5F2A8A

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.casella[1].xml	
SHA-512:	E79A92461E5A812C742EDA11B5F8B27338F8D531D2B7BECA1C627101396F74E7D440A3BDD03705E9CD2F6F28427465581FA6749BE5BF33FE470167B421EDC14F
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1085396704" htime="30884126" /></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1085396704" htime="30884126" /><item name="61870c77-2e72-45dc-9f17-2f74952d866e_override_site_id" value="" ltime="1095276704" htime="30884126" /></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1085396704" htime="30884126" /><item name="61870c77-2e72-45dc-9f17-2f74952d866e_override_site_id" value="" ltime="1095276704" htime="30884126" /><item name="rl_initial_referrer" value="" ltime="1108236704" htime="30884126" /><item name="rl_initial_page_uri" value="http://www.casella.com/" ltime="1108236704" htime="30884126" /></root><root><item name="capture_base_site_id" value="61870c77-2e72-45dc-9f17-2f74952d866e" ltime="1085396704" htime="30884126" /><item name="61870c77-2e72-45dc-9f17-2f74952d866e_override_site_

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\61870c77-2e72-45dc-9f17-2f74952d866e.rlets[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	31687
Entropy (8bit):	4.864381787482574
Encrypted:	false
SSDEEP:	768:LwrDegARvJJVMCnB/AvcEV2XVI2+88PVPmP6PoP4PWFEube7:LwrDegARvJJVMCnB/AvcEV2XVI2+88Pd
MD5:	64DC86288FB68A4A727183ACB719BA93
SHA1:	354475FDB46D4356D8FE7E785DBB660A516B4F00
SHA-256:	90A005D3BC3245C3CD9896B592C3D3C7B55C9A0C0567B980A90B003E5CD77115
SHA-512:	DA943DEB36F4B3B43609C13B12F552E3C3D2FFF92810743128CE8F7AA9D8BEE4ED76E8DC3B1901506F966E56B9FD7268AF9D69FABFD21D5D76814BBEEA3ED18C
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="test" value="test" ltime="1094486704" htime="30884126" /></root><root><item name="test" value="test" ltime="1094486704" htime="30884126" /><item name="override_site_id" value="" ltime="1095276704" htime="30884126" /></root><root><item name="test" value="test" ltime="1094486704" htime="30884126" /><item name="override_site_id" value="" ltime="1095276704" htime="30884126" /><item name="bot_type" value="" ltime="1109236704" htime="30884126" /></root><root><item name="test" value="test" ltime="1094486704" htime="30884126" /><item name="override_site_id" value="" ltime="1095276704" htime="30884126" /><item name="bot_type" value="" ltime="1109236704" htime="30884126" /><item name="history_campaign" value="" ltime="1109276704" htime="30884126" /><item name="history_referrer_type" value="DIRECT" ltime="1109276704" htime="30884126" /><item name="last_activity_at" value="1620157624466" ltime="1109276704" htime="30884126" /><item name="visitor_id" value="95fa6a68-9b

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7BEDC59C-AD11-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8486438816955302
Encrypted:	false
SSDEEP:	192:ruZ1Zl2ZW/tHifXPxzMUpBsDDZsfNPMjX:r67folgeKWcy
MD5:	2FF081EB23FB28589FAE3AB28240CD9D
SHA1:	7DE9564A097A11D86FA50AC4C7FF0263FAC98146
SHA-256:	E04EC05A2DDCCD507C96C3545870C81F771D27B5E177F942D8CE2E52D31D825D
SHA-512:	24732F26E4587EE88C50B7CB77DAE5D6EECD31EFC541B6013DFE5055E7DC8D7F382F106EF88679C14FB338787BE7C4BE3FD0F24CBFA75FF7548048096B64610
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	199758
Entropy (8bit):	2.763898779842383
Encrypted:	false
SSDEEP:	384:ruCk0y4wlZTVeflDHjch9+LIDaWu1dXu+cEgbkhIoc/IHvpU7+3DkCvLzUR3oSnV:HD3Md
MD5:	9E7B92665766C4917A166286AA05FBB5
SHA1:	4EE0014B0FC15D3ECF9863D8D51E5EC1596216FC
SHA-256:	85EE934B07E6FC1CA94281ECFDEA5FFB6C2F5F3D37E11204836ED364F80339BE
SHA-512:	46A63B3A41D835F2F1318AFC0D9BD07F7D8A2A3C2F89388B77BC8BFE3A5ABE6631B7A158744929B4679C5EE37EAC2FA925F300711B1E1B2F31F21EEDB5A5C212
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7BEDC59E-AD11-11EB-90EB-ECF4BBEA1588}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{82CFA500-AD11-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5641093935758295
Encrypted:	false
SSDEEP:	48:Iw8GcprVGwpa0G4pQTGrapbSaZGQpK0G7HpRvaTGIpG:rgZ/QE63BSazA/TveA
MD5:	34C186C39F45211685DEEF420293FED0
SHA1:	9902A5293523189905EF398F3654D2030DD042EF
SHA-256:	C0FBFF7DA75EBDB53C6B74740985F472CEBD9AFC3208D67574B3BAD06E761906
SHA-512:	A9D93E5AE594F9A602954FB90BD11D26AF17192B6815CEC0E926C079CEDF9243F0B22ED343ABC6B73DFFAFAE7AD7982011FE2D0C10A88E61AEFDD9761DEE6B0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3512
Entropy (8bit):	6.10202470888679
Encrypted:	false
SSDEEP:	96:uxoPBjTpGWoabmG8CL3uSTdfAApixoPBjTpY:uxov93jQxoY
MD5:	BBA3FCF7B4C0C25B92FE15F86F1AAC26
SHA1:	EE9252B4BF13CB03628ED01DAD87285B317FCDF0
SHA-256:	F5A29436F76DE4B2E601557E1C9BAA4D84D1FC22D599C458FC373D87FA031F0E
SHA-512:	B9543748CB0B19C1C46AEF0B7BAA75A073D9D506FECB767C0C55CC7E51AFE2707A2FE9BE37BF7E733C7A8485840326CCB2F5FCCC5F8A3F799DF6BF9ED1762BB
Malicious:	false
Reputation:	low
Preview:	l.h.t.t.p.:./.w.w.w...c.a.s.e.l.l.a...c.o.m./.t.h.e.m.e.s./.c.u.s.t.o.m./.c.a.s.e.l.l.a./.i./.f.a.v.i.c.o.n.s./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.-....PNG.....IHDR... ... .D.....gAMA.....a....cHRM..z&.....u0...`..:....p..Q<....PLTE.+Ap.....8M...Xq..&>.....Idt.9N:Wj....2G.+B.....?S/N`(H\.1F.8M.8M.8M.:O.:O.<P.<P.=R.>R.<Q.....'=.....&=:Xi.....Yq.....'>.+Ax.....Nhx.&=.&=....6.{...9tRNS.....bKGD:N.....pHYs.....L"M.....tIME.....0.....IDAT8.c.$.....+`fa.(`....A.8p.[q.R.E...<.|.....=&(.[.08lD.).%.@L..$.+@..L..R.2.r...J.....W...R..[.....V:.zVx.....)0.'ZC..F.`.&.f....~...n.0.O....%tEXtdate:create.2017-01-03T16:48:18+01:008.qd...%tEXtdate:modify.2017-01-03T16:48:18+01:00I.....tEXtSoftware.www.inkscape.org..<....WzTXtRaw profile type iptc..x.....qV((.O..I.R..#..c..#.K.... D.4.d.#.T .....H.J.....t.B5.....IEND.B`. ... .`.....`....&.h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\111[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2357
Entropy (8bit):	5.1447703901082225
Encrypted:	false
SSDEEP:	48:cxkdCpj2xygvI/AVk6dMdSsxXXdul5x3zrjEJxMqxL:zIj2x9IIVlMSa9uV3HW1L
MD5:	5A71F8658593419AB94D74DE35A0D2E2
SHA1:	FD8A53D51134177CBFF9C64EC2DEF3F0BDBDAB8D
SHA-256:	DBD4A7532356753472D2D4EFDAB033D1BBB02C5BDE13EAE9DCC3EA5F028E42B6
SHA-512:	1705A4739B3E9A554BEBD81F993FC8E8A23AC7FA0D24EA4B641A74FA5591B33B608999C9C313A25B0475D082A5F8F9D46AE9137E0A6A9CB2D82388AC95E9FC63
Malicious:	false
Reputation:	low
IE Cache URL:	http://apps-cdn.twinesocial.com/images/emoji/111.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\111[1].svg	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg xmlns:svg="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/2000/svg" version="1.1" viewBox="0 0 47.5 47.5" style="enable-background:new 0 0 47.5 47.5;" id="svg2" xml:space="preserve"><defs id="defs6"><clipPath id="clipPath18"><path d="M 0,38 38,38 38,0 0,0 0,38 z" id="path20"/></clipPath></defs><g transform="matrix(1.25,0,0,-1.25,0,47.5)" id="g12"><g id="g14"><g clip-path="url(#clipPath18)" id="g16"><g transform="translate(34.3047,19.6636)" id="g22"><path d="M 0,0 C 0,0 1.132,1.65 -0.519,2.781 -2.168,3.912 -3.299,2.262 -3.299,2.262 L -8.55,-5.396 c -0.18,0.302 -0.379,0.6 -0.599,0.894 l 7.288,10.629 c 0,0 1.131,1.649 -0.519,2.78 -1.649,1.132 -2.78,-0.518 -2.78,-0.518 l -6.856,-9.997 c -0.255,0.209 -0.515,0.417 -0.785,0.622 l 7.947,11.59 c 0,0 1.131,1.649 -0.518,2.78 -1.649,1.132 -2.78,-0.518 -2.78,-0.518 L -16.1,1.277 c -0.292,0.18 -0.581,0.335 -0.87,0.498 l 7.427,10.832 c 0,0 1.131,1.649 -0.519,2.78 -1.649,1.132 -2.78,-0.5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1612366471[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	502533
Entropy (8bit):	5.484857938704484
Encrypted:	false
SSDEEP:	6144:jJq17hbvca98Hrt1cSBnEDFKpfdQCXSvecF3:UbA6FGWKA
MD5:	9B6B9BC3C915179C675CEE7DB6A85752
SHA1:	1C0D7FC0C331612F3BA4E930463055822A68B796
SHA-256:	23611817E66BCB3E89E566E2BBD6F9D012FB08B460F1E07679384D86DF8BCD04
SHA-512:	45727B49544334045F2F92928037FDE190466DB1212403D470F9C6781FB3825C7E52CEF37D1CD745191DE4352BB9428141310523572AFA50D28C967EAEE7EC61
Malicious:	false
Reputation:	low
IE Cache URL:	http://apps-cdn.twinesocial.com/js-min/files/player%252Fbugsnag.js+player%252Fjquery-1.11.1.min.js+player%252Fselect2.min.js+player%252Fjquery-easing-1.3.js+player%252Fjquery.timeago.js+player%252Fbootstrap-3.1.1.min.js+player%252Fisotope.pkgd.min.js+player%252Fjquery.lazy.min.js+player%252FjMinEmoji-SVG.min.js+player%252Ftheme-base.js+player%252Ftheme-base-utility.js+player%252Ftheme-base-toolbar.js+player%252Ftheme-base-fx.js+player%252Ftheme-base-manage.js+player%252FisInViewport.min.js+player%252FAnimOnScroll.js+player%252Fmodernizr.custom.js+player%252Fhandlebars.min.js+player%252Ftheme%252Fclassic/v/2.21/t/1612366471.js
Preview:	// player/bugsnag.js.!function(a,b){function c(a,b){try{if("function"!=typeof a)return a;if(!a.bugsnag){var c=e();a.bugsnag=function(d){if(b&&b.eventHandler&&(u=d),v=c,!y){var e=a.apply(this,arguments);return v=null,e}try{return a.apply(this,arguments)}catch(f){throw l("autoNotify",!0)&&(x.notifyException(f,null,null,"error"),s()),f}finally{v=null}},a.bugsnag.bugsnag=a.bugsnag}return a.bugsnag}catch(d){return a}}function d(){B=!1}function e(){var a=document.currentScript||v;if(!a&&B){var b=document.scripts||document.getElementsByTagName("script");a=b[b.length-1]}return a}function f(a){var b=e();b&&(a.script={src:b.src,content:l("inlineScript",!0)?b.innerHTML:""})}function g(b){var c=l("disableLog"),d=a.console;void 0===d||void 0===d.log||c||d.log("[Bugsnag] "+b)}function h(b,c,d){if(d>=5)return encodeURIComponent(c)+"=[RECURSIVE]";d=d+1||1;try{if(a.Node&&b instanceof a.Node)return encodeURIComponent(c)+"="+encodeURIComponent(r(b));var e=[];for(var f in b)if(b.hasOwnProperty(f)&&null!=f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\170581839_10159677912488888_3092895498031908587_n[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 50 x 50, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	2640
Entropy (8bit):	7.883167737695746
Encrypted:	false
SSDEEP:	48:c6kemZCOldISPIgM+9iNBIkfr8YcRgnwJ1u5PtEy37lGPmK:ByLI59r8B+n7EPV
MD5:	266A6E4C7A662C7C9C6C8097CB4A86A7
SHA1:	9540D794F99234C9141758B7DF3744A4A2A2E5E0
SHA-256:	1CE6EA57D15B8C472484E9CD86DB3856067AD2829EE5283D69B2718A7FCE67F8
SHA-512:	E72BE9ED1DAE7527EA85245BFC50005613824AEEDA84DE7598279CFFC3323AD79E673C100A3C3BBF13CC9B47E96DDF14A1A07D8FCA49C488D649208754165CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scontent-frx5-1.xx.fbcdn.net/v/t1.6435-1/cp0/p50x50/170581839_10159677912488888_3092895498031908587_n.png?_nc_cat=111&ccb=1-3&_nc_sid=dbb9e7&_nc_ohc=8dXRoCtschIAX9A_vJW&_nc_ht=scontent-frx5-1.xx&tp=30&oh=18cfa11f6062b78d1049627f27680a83&oe=60B699CC
Preview:	.PNG.....IHDR...2...2.....].....sRGB...,....SzTXtRaw profile type iptc.....@...>....u.B.....]...X.L.w&Hx|..VK(.p...jsq._....?.....IDATX..i.....1.3=.wv.....&6`.....B...aD..HN.....("..8...B..".A.....6.....\.]{...v.~U.0.....K...Z..~O...zU.....7...<..y.3..Xgb....Q,5....I.#..@.....fM,.....hc._8q^i.;Py....O.R.....x.u...L...y...C.!.<.Q.e.....yw.~..Q...W....<Z..K...2...].-q0.V...E.....~.8.mZ,.....n.....1..@.X%Kg...../..0K.....[..z.2.< ..T43Z.3#...1!.1.q..^...p.T.%.XV..g.....|S...?..'...]{...R..M.8.{dy{[...j..a..;.t.w.-...c....d*M...;/...m.ke..B..y...5kK{-.X(n..yl(...w.).^;..I.'j.U..d.(Z..|n._.....Y.N.3D..S.?....>.+".B...f...3....z.5.....a3.....WW..w....._[.NO.@O.@..p2...c.l...P.3...H&.L...L.._x}..w?P.....'....Ew=.|.....G.hl..L.....2.x<.....s`.m7.46.....8.d..^...C.x...h.@mMu{[s*..b|x....V.Y.....2.+/.7k..|.o...1pWO....c.DsS..+..~..B...Z....+....;...mZ.k.kp..._.....a.....,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\176597167_780408019282225_3124021654920406254_n[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, progressive, precision 8, 1280x720, frames 3
Category:	downloaded
Size (bytes):	42280
Entropy (8bit):	7.944422037263365
Encrypted:	false
SSDEEP:	768:CYysdxQohNScNYYD3Rab25iwdbVeTuujllN6Sn1KtHHpx+LAd6SxbWOA8qs/:C2xQohAcNLxxVmdl//1+n/+LVeW38d
MD5:	D58C361FE70620C74E735166CABF6CA6
SHA1:	E4FC1061FF8811D255CBA48378A43C5E25687F54
SHA-256:	FF11C4B3735D878AE70334D745737D7C64B7F50EB19917E1E48AB3B72D7C3B8C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\176597167_780408019282225_3124021654920406254_n[1].jpg	
SHA-512:	254265F82694CA4D76254B67517F40D89E3CCBF46C02CB0ABC6609E488426C2724389CE12DA3E8464DF289D6A7F8E06AD8121A31DF0348C2D3E8565F0A27A83(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scontent-iad3-1.xx.fbcdn.net/v/t15.5256-10/176597167_780408019282225_3124021654920406254_n.jpg?_nc_cat=106&ccb=1-3&_nc_sid=ad6a45&_nc_ohc=i36gvYeY-FoAX9IBK-l&_nc_ht=scontent-iad3-1.xx&oh=9417d9dfa58540bdb64ff130ced49cee&oe=60B43256
Preview:	......ICC_PROFILE.....mntrRGB XYZ .....$..acsp.....-....).=..U.xB...9.....desc...D...ybXYZ.....bTRC.....dmdd.....gX YZ...h....gTRC.....lumi...\|....meas.....$bkpt.....rXYZ.....rTRC.....tech.....vued.....wtpt...p....cprt.....7chad.....,desc.....sRGB IEC61966-2-1 black scaled..... .....XYZ .....$.....curv.....#.(.-.2.7.;.@.E.J.O.T.Y.^.c.h.m.r.w.|.....%.+.2.8 .>.E.L.R.Y.`.g.n.u.|.....&./.8.A.K.T.].g.q.z.....!.-.8.C.O.Z.f.r.~..... .-.;.H.U.c.q.~.....+.:.I.X.g.w.....'.7.H.Y .j.{.....+.=.O.a.t.....2.F.Z.n.....%.:.O.d.y.....'.=.T.j.....".9.Q.i.....*.C.\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\181086922_10159734185388888_162057070642722993_n[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 720x540, frames 3
Category:	downloaded
Size (bytes):	72205
Entropy (8bit):	7.97824052383283
Encrypted:	false
SSDEEP:	1536:DhDB9ffn5ZkkRMo1FTvwgS5VhMKDHOn2yjDPIb9uKW8FNb:5B9f8iMoHsgSzOn2MDPGwIFNb
MD5:	E986655CABCB5273E0FA107ACB87FEA8
SHA1:	2F94D275F503909C6B4EDE3E1E5E56A9A9AA8A80
SHA-256:	068A906E26814252409BA2B1D98CBD7E6CBDA9960102435F2563FDEDB83B794E
SHA-512:	5BA2C74275B1E854D0122E5E2E5A9A73FD1A0A76B5B096D8B0D91F8EC5D6BE0F0F6B0B72DFD1AFCC5FAF88DCE15997445DB6800AC07F9A35966B37175060ED 99
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scontent-iad3-1.xx.fbcdn.net/v/t1.6435-0/p180x540/181086922_10159734185388888_162057070642722993_n.jpg?_nc_cat=107&ccb=1-3&_nc_sid=110474&_nc_ohc=DjNS5gRWOIwAX-NA2fQ&_nc_ht=scontent-iad3-1.xx&tp=6&oh=d4f4e52e1efe98f0eefe92ada29216b0&oe=60B1C57B
Preview:	......JFIF.....Photoshop 3.0.8BIM.....h..(.bFBMD0a000a700100008a18000040410000c8440000b2480000c673000096ac00004bb100009eb60000d9bb00000d1a0 100....C.....%...#... , #&')*)..-0-(0%()(...C.....(...(((((((

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\350[1].svg	
SHA1:	4A587F24F99552FC8FF4EA176A45260495845443
SHA-256:	3AE7D3FC34C1CD676A45BC2C72C3D1BE265D227071C6819E72BFDDA3FAD7E90B
SHA-512:	9EB9FD110ABECAABCC43081C10C79D6C7C6DB998FD52CB39C908B27E37E2066025C2190DF88675B7C8F8A9C01DF27A585B614EDB7260493264A7A5313193C12
Malicious:	false
Reputation:	low
IE Cache URL:	http://apps-cdn.twinesocial.com/images/emoji/350.svg
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg xmlns:svg="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/2000/svg" version="1.1" viewBox="0 0 47.5 47.5" style="enable-background:new 0 0 47.5 47.5;" id="svg2" xml:space="preserve"><defs id="defs6"><clipPath id="clipPath18"><path d="M 0,38 38,38 38,0 0,0 0,38 z" id="path20"/></clipPath></defs><g transform="matrix(1.25,0,0,-1.25,0,47.5)" id="g12"><g id="g14"><g clip-path="url(#clipPath18)" id="g16"><g transform="translate(15,8)" id="g22"><path d="M 0,0 C -2.209,0 -4,1.791 -4,4 -4,6.209 -2.209,8 0,8 2.209,8 4,6.209 4,4 4,1.791 2.209,0 0,0 m 0,10 c -3.313,0 -6,-2.687 -6,-6 0,-3.313 2.687,-6 6,-6 3.313,0 6,2.687 6,6 0,3.313 -2.687,6 -6,6" id="path24" style="fill:#3b88c3;fill-opacity:1;fill-rule:nonzero;stroke:none"/></g><g transform="translate(2.78 32,22.9766)" id="g26"><path d="m 0,0 0,-0.021 c -1.001,-0.218 -1.783,-1.895 -1.783,-3.956 0,-2.06 0.782,-3.737 1.783,-3.956 l 0,-0.02 28.701,-7.972 0,23.884 L 0,0 z" id="path28" st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\475[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3847
Entropy (8bit):	5.171594213317656
Encrypted:	false
SSDEEP:	48:cxkdCAFvKH8NaJJthRWC2EjSwmzNSCZbesUakpHPTGHaL/PElJFhqizkOW5:zn4cN7CTSBNSCfUJpHSi/P86
MD5:	CE071A596B6D16E8B1C0E6121661B015
SHA1:	28429EC3F3A53A8F8686518B097656B49D3BB754
SHA-256:	5A6616BDF46D37FB2551818A4941E3D788DF96E57E024ADFB4A4F072E52349F5
SHA-512:	096179B9D0AEA31E677DFE3C4582F9FC1A86FA290B40D05D8CA7DF74AA811DE4E7B2B1336CD6B79FAEED1B3918D4BCD129ADFA0264974A9F8A865E3C42CED82E
Malicious:	false
Reputation:	low
IE Cache URL:	http://apps-cdn.twinesocial.com/images/emoji/475.svg
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg xmlns:svg="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/2000/svg" version="1.1" viewBox="0 0 47.5 47.5" style="enable-background:new 0 0 47.5 47.5;" id="svg2" xml:space="preserve"><defs id="defs6"><clipPath id="clipPath18"><path d="M 0,38 38,38 38,0 0,0 0,38 z" id="path20"/></clipPath></defs><g transform="matrix(1.25,0,0,-1.25,0,47.5)" id="g12"><g id="g14"><g clip-path="url(#clipPath18)" id="g16"><g transform="translate(9,21)" id="g22"><path d="m 0,0 c -0.552,0 -1,0.448 -1,1 l 0,11 c 0,0.552 0.448,1 1,1 0.552,0 1,-0.448 1,-1 L 1,1 C 1,0.448 0.552,0 0,0" id="path24" style="fill:#ccd6dd;fill-opacity:1;fill-rule:nonzero;stroke:none"/></g><g transform="translate(3,4)" id="g26"><path d="M 0,0 C 0,2.236 4,6 7,6 L 7,1 C 6,1 3,0 2,-1 1,-2 0,-1 0,0" id="path28" style="fill:#3b88c3;fill-opacity:1;fill-rule:nonzero;stroke:none"/></g><g transform="translate(17,4)" id="g30"><path d="m 0,0 c 0,2.236 -4,6 -7,6 l 0,-5 c 1,0 4,-1 5,-2 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZY4lCds18l[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19212, version 1.1
Category:	downloaded
Size (bytes):	19212
Entropy (8bit):	7.974755958403984
Encrypted:	false
SSDEEP:	384:vyrzxrRnuXB6wgkFx4rjY+dx47uhGTJWXj1oHjt3DPl4MCX6mQW1gZS9pMgINptt:vkr8XB6XW43/LyJWXj1oHjIMw6Ug89pS
MD5:	C13797BD5E320111CF0AF5C140AD9EE5
SHA1:	009FBB0574E44FCAE9B67AF50F397B40A5B3CDAA
SHA-256:	CA250667A898B5996D8A46DF440CE42A44A2B6C1016A84094EB237E22C44FBC1
SHA-512:	B7A94B34CD16DE1CCFFAD7BF08843DE259453C22428161D53E66965D358E1187A972562C4BDBD755A73B0B45A8FC17E1208DABE08153E6AE2E0A612DEB6BBE1B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xKwdSBYKcSV-LCoeQqfX1RYOo3qPZY4lCds18l.woff
Preview:	wOFF.....K.....|.....GDEF.....0...:.\..GPOS.....b./.aGSUB.....#.#.OS/2.....Y...`[.u.cmap...8...k.....Icvt .....*...*.X..fpgm.....s.Y.7gasp.....glyf.....5...d..."Ehead..A....6...6....hhea..B....#...$.9..hmtx..B4...M...D.m".loca..D.....$Uxn.maxp..F.... ... .+.Wname..F....F....a.y.post..H.....prep..J....S...VS..::x.....0.....v@.C.=..xz.>....ZY...x..3..A.....6c.N..m.....r..A...b..|.....[.!D.L\2..e.....S..#...T)...B46gp.P..2...V...Z.PKm.3.2p.9.....)v..f..c...F.S....[4..{O.....w..>..{..O....}.....To.....5..EG~.oyX..`.li..e=...&.r...<....b.(el.7{..A.`h...e..')..&&)..B.....)#+.r.#/Q...(1J..2U.V.$.%A-1...%A...T.4.7..K...R....!:I...U...1H.....".h.3...Og...,".b..g9+H.M.. o%.....b..;hBCx..@..Da.Tq.....*.(...."..... .....D....'..QQ.Q.4.n....8.....]..&z{f.....y..7...Cb.;.K.m.)K..Q.5...9.ju..]zh.!.A..p...M..a..?...`..6...5.G...3..D.....C{...y.)G<...w-.2....|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\747[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4303
Entropy (8bit):	4.983979961659166
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\747[1].svg	
SSDEEP:	96:z4z+Rlw1m3jShCRoehpRtBVj8JY7sTQt45587uVSnL:8+RlDGEhpjfj4Ui+iU
MD5:	D1B5BF793F3DF67A091646E45E0C4FED
SHA1:	814C3BD2DC47CF9BE30D775844038830495D87EE
SHA-256:	9E55A202DA52704AA5E84FCC7C35F52460097D97672942D7025EFFBF4658DE6C
SHA-512:	DBBF6342EB4AE108E8CA34953C6243B85F419EB97FE61015705A4C650086D7787159ED7B9DE1C09DFD7000DC8E1E0449EA3F5513D4EA6986411B84B04DA08A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://apps-cdn.twinesocial.com/images/emoji/747.svg
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?><svg xmlns:svg="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/2000/svg" version="1.1" viewBox="0 0 47.5 47.5" style="enable-background:new 0 0 47.5 47.5;" id="svg2" xml:space="preserve"><defs id="defs6"><clipPath id="clipPath18"><path d="M 0,38 38,38 38,0 0,0 0,38 z" id="path20"/></clipPath></defs><g transform="matrix(1.25,0,0,-1.25,0,47.5)" id="g12"><g id="g14"><g clip-path="url(#clipPath18)" id="g16"><g transform="translate(31.001,8)" id="g22"><path d="m 0,0 c -0.348,0 -0.685,0.181 -0.869,0.504 l -4.235,6.975 c -0.275,0.48 -0.167,1.08 0.312,1.354 l 4.958,3 C 0.322,11.923 0.662,12 0.83,12 1.178,12 1.502,11.802 1.687,11.479 L 4.794,6.357 4.958,4.125 C 5.232,3.646 4,2.941 3.521,2.667 L 0.495,0.132 C 0.339,0.042 0.168,0 0,0" id="path24" style="fill:#3e721d;fill-opacity:1;fill-rule:nonzero;stroke:none"/></g><g transform="translate(24,5)" id="g26"><path d="m 0,0 c -0.553,0 -1,0.447 -1,1 l 0,6 c 0,0.553 0.447,1 1,1 l 10,0 c 1.85,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-CurbsidePickup-1900x960[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 75", baseline, precision 8, 480x384, frames 3
Category:	downloaded
Size (bytes):	29167
Entropy (8bit):	7.960392640140513
Encrypted:	false
SSDEEP:	768:e32fwRFRlBNZjRWvyQBLjIRG8AamiaQx9Nl9kpUZ7EH:e3awRrNZjTQBLjIRxva4NlzyH
MD5:	170060025134070DAA928D61C4667151
SHA1:	F6C4DEEF9F1AB31DE55D64D8FF9D3D5665DBB76C
SHA-256:	2BDD9E2D5EDE74AF956349CE407A7A0CE9F5234B15DD59C2848D30C51D93F381
SHA-512:	4E45ED721AD5E5E5AF0133A19CACD38023C26B6BBC8691042876EDD508597FD83540AAE9BC9996C87F61150C12EFC63BAD13C4AB507C150DE52E00A516E704 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/480x384/public/2016-11/BANNER-CurbsidePickup-1900x960.jpg?h=7a8a8cdf&itok=9P7rGhj3
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 75....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!22222222222 2222222222222222222222222222222222222222..... "..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTU VWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz.....?...)(. Z)(...4.P..IQ\\.k..g...'.&.....=...[..ee...P{...U..T.:d.I..&;4f..c.4f...-..P..IE.-%.P.E.P ..IE.-..P..E..QE..QIK@..f.....).QFi(...(.....(.....Q@.%.P.-\.D.>....t...f.}].....R...Y..._%9..UD}.k(5(j..EM...5B..C.....a.kCNA":.;b....?z....._..i.....q.....V..W.....`.H..2.....g.*+..... ....Z..L..].

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-Drivers&Mechanics-1900x960[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 480 x 384, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	296598
Entropy (8bit):	**7.996560621800548**
Encrypted:	**true**
SSDEEP:	6144:ZOcMjmclLDN+M5piS6TYEpD5K/DYo71Nzw+Ay7HWr+CwIWLOBvv:ZFMjXlHb5pGHp9K/D1nk+FarHWO5v
MD5:	22E273E057359BC337E2C6E718D0352B
SHA1:	76EE5FC5AD8BF3ED7F025EA1AF61D045017B5182
SHA-256:	DBD300C3EE324FE4DAD786ACA252655D670387105F78ED00926E4DDDEB57A318
SHA-512:	415E076BC1724663264D2F8ECF8210B2480BCD82DA04CEEFF447A6CABB1D2783195EA0CDFF5101873A9541B33A71D02A3D9C7236E048482E7BBE63671AFDC7E 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/480x384/public/2018-06/BANNER-Drivers%26Mechanics-1900x960.png?h=7a8a8cdf&itok=pdz2vuKB
Preview:	.PNG.....IHDR.....u .... .IDATx...k.n.U.6.....D7..&.s'.Fr.b.....W....;.%)W.r).XT.J.....IL.G6...`."HBHj.....>{..c.....N..e.u..1/k.....)...@`^...c....."..@".V..3.+..@f..M...0. j....4..?...8.}.....@d....2.....}..R..o.."..y"V o9.....C..c..g,.....N.M..I..5.k3.....S...g..xF..?.A.)8.Df.X..H...+p;O..Xu_D.G..1..y&.QmF..D.G.L../"...XKC;s&...m...Do.....I.@.o.j...CD` ..W.Us.....6W....~...../.....uM}.\...N..IJQ(...%..5.n..B._m.gO...g.Lf.....L.|L....4.a.....7X..lx}....:/....Vl.^.n..@.....f.h..N.F.....X1..[.....\&y..q.t.....j..M...VP..7./.....9..y.y& ..K.d....#.....X..E.3....j/..(..$..!.iAv.b..>....1...S.YG_.....9...../..Zk.`.2..0.@m.Mr...L.C:D.....c@..-....A:p.."..{....c.v.....8....,..._]...h....*i.G..(."0.dhT..`I...ZJ...8i.A.....z..q..i.F....:}... .H.-./#..-.=...A..X.I]7..qF.X.'.I&...D8...W#.t$L.....`..-.k...e...+.....h...4#...1`.'b.....-#.YrWc...;.Z.].u3*.7LU..)...J.3.]...J.K[.)...E 8...8)5&.$.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-RecycleRight-1900x960[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 480x384, frames 3
Category:	downloaded
Size (bytes):	156044
Entropy (8bit):	7.952888574563787

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-RecycleRight-1900x960[1].jpg	
Encrypted:	false
SSDEEP:	3072:xe53zREFU1qRnUM1DusBlmrL+PYjojkXjRIsvz7K8s/9ea2DjB:W3tEaGUM1DJ1Moj4IM7K8y2DjB
MD5:	F1EEF35D2611AFF26180FE9591A0ECFA
SHA1:	A361702E3C486DD0C2F3CC56EAC24996E45ECD22
SHA-256:	92AE250606EA0CDAD6C9114D075F8946980B86D03FF67D903F8CA5C8A1956F05
SHA-512:	A1E20A1B42611AB2F3843A0D1D2F255A6C689AF83F2C9481DDF8FB75BBEF0BC1AEE0BA0F4AA5BA9B04377A8A9C5011A67CF06A7B65130F16E0CFFA819C8E2B5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/480x384/public/2018-03/BANNER-RecycleRight-1900x960.jpg?h=7a8a8cdf&itok=OVikH09Q
Preview:	......JFIF.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....d.>.vS.E...4...8.y.....A"...s...1....aT.?.#.F.2....8...?...8.t.....u....#..7..k....<..88'..#.P.YF.3.A...'.....h.7e.8..x..q.A.z`.==()A.5o...lX.q...>....;J ...4.H9..c....P;z....Fr!....8 ...=~`...9.....c..G8'.,....{'.E...._...I.....N....$.....q.....''h..O....?..Ny4.$.....r?...b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-SustainabilityReport20-1900x960[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 480x384, frames 3
Category:	downloaded
Size (bytes):	196578
Entropy (8bit):	7.93780943952382
Encrypted:	false
SSDEEP:	3072:HXVHa/t4M46gXESc+AX1jPgPySf/kkhwNJFVB7CiO9vwQoyZnXYBQnM5QtTUGdBh:3VH2SfAXRY9f/kawNJ5OuCBXY+XBBtbF
MD5:	43A302CEE576C136EB9C1FE9D1E05F1B
SHA1:	A4B7397623C9F925F35E2E212EA7F1DC9FCF77CE
SHA-256:	111983E82EBE1183CA440E201D647D8A9B614812AA05D66638C74AD603891382
SHA-512:	14326FE538C3C3AAB9BD5B1340B645AC0B48554974410BEC8DD3E95F0D9C6813F72ED4376AD6737C6DFFFF015BD382F4E295B9ED4F3895973DF3111A4B4BF9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/480x384/public/2021-01/BANNER-SustainabilityReport20-1900x960.jpg?h=7a8a8cdf&itok=X4pFSupk
Preview:	......JFIF.....`.`.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....[..no.O.|8.m.....Ud2.i.*..3.....M.....-....x....*.X."..:..$+;.h.JGn..J.Ir...n]f.e.....?S.....X...^.?....v././.B.K.b.....Ciux-....''...O..k$..&...x.....n...Y....R.... O:..,...a..w...5..E.A..9.....`...b..^j.|V..d.J.<<UiN....RP.9.....r.%.y.....`1xY.b.O....F*.I/r..''i^.n.R..}..^M..H.w.Zd.)./4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-SustainabilityReport20-1900x960[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 768x614, frames 3
Category:	downloaded
Size (bytes):	466195
Entropy (8bit):	7.949080438388158
Encrypted:	false
SSDEEP:	6144:W/r47Jmqcx3qt26uFuEwFUoTK0B3BPZsfBZV32GsXhQA7e6hSfP7bYX95Z2J96en:f7Jm3qt268uEr6F/ELV3XI7r8n7sX89J
MD5:	E5BD6091F571334613B3E8D4A786FF5C
SHA1:	8A60776337E938A5CCC1B66D6E4B2292FFEC388C
SHA-256:	61EC07D4608A5175F4D8D6DAA39745E8E3EEBB4686932C70F7280158B93783D9
SHA-512:	73F66B5AAB7D61475513211D001467AAE7C03C4F085F68598D2993EE9FB11F221A04B0BFDC22A3B654F6EFBA45A1D380359EE410A2AEE455C547AF0EAE250692
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/768x614/public/2021-01/BANNER-SustainabilityReport20-1900x960.jpg?h=7a8a8cdf&itok=Ia_fF50X
Preview:	......JFIF.....`.`.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....f...."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....}....Y.G.Y..a..C.kP_\.....J..C,x.._q`z.=...f...Z..'.U.]..y...{Geo5..R...6....Y..K.Ic...+&..^.M...y...zM..... ..a&.n4..0&.+...#.Kn.`.....lt.3R...0\..... .$I..-QC.Y<..om...eg....D.t.\%...9!...V'....kEN2..R..B.6..Fu'..i.O.8..'.....K.(.*SnQjr.V..(FJ...,%h7....,...,d.....t..u....i.Dc[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-ZS-2-1900x960[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 480x384, frames 3
Category:	downloaded
Size (bytes):	199185
Entropy (8bit):	7.948897086375355
Encrypted:	false
SSDEEP:	6144:DcsrX8qr603K1PFlCu8NXPHZJKFSkw8s9A:gok0aFrCLXP5YFnKA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BANNER-ZS-2-1900x960[1].jpg	
MD5:	48010898EF61B92A25CBB7F80571E0CB
SHA1:	5C4FEAC3C38B9A4221E2FFD4D7F4D1C57C19FE27
SHA-256:	D8FD1C704F84E286AE0E039A3AD0EF62937033E9527404B6FBB67FDCDAB52803
SHA-512:	51F18EB1FCF77AB973ED8E234B87E24D4560F37D8FE98F381DB29030C18614B616D749E00367A65032C3030BD9D06EE34A1788A76ECC28D004B563571F95AFB4
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/480x384/public/2017-02/BANNER-ZS-2-1900x960.jpg?h=7a8a8cdf&itok=fdBWRZI0
Preview:	......JFIF.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..L..k.>..o....Y.d[..w..fX...%...Xn.....y."f...5..._..x.C....X...Nd...,q...[.....kb....z.Vg.4.I+.... .,..t..kZ#}.6D.K.aI<.....%.Kv.c.E.6.Z.....?.U..Y..Ar..{.C..eo} v.Q[I...5.>.....A<..B.K'...mba.&..Z.tVM..Vm.....A.EA.Y.^.[.....g.\..N.u.".E.h...[y..[..D.{.c.InZ(.?..M.'I!..].s....Q...c.!..4.K...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Enroll[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 87a, 52 x 19
Category:	downloaded
Size (bytes):	1410
Entropy (8bit):	7.198100774838102
Encrypted:	false
SSDEEP:	24:IKjreoAX1BthLFyQgtZcGflcSeLUwTmYsEYz7pir0pC5:/uoAX1BnHgt6Sem+YBiw6
MD5:	3F3599581B8F9C8514F3C8D86B172214
SHA1:	5C994AF0C665AF75628908F3D4D0A6D655E970B6
SHA-256:	4B08DE83E867054BBC53BBD78C280D83FCBF61DEA19D56AF1373C9A1FA7BBD2F
SHA-512:	5BE3F959AACE550E722B7A0E2748D05FBD0443E3873FB099C5A286DCF4258F7E44980AB08672A48625DEB65666D25642816DEEEE85AF16B6D68A63AB18B70CA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure3.i-doxs.net/casella/images/Enroll.gif
Preview:	GIF87a4.....ZGKTGKUGKVFKYGL\KMSHN\HO_MPWRU[UWYGObKRcKSiW[eV[h]_aU^uR^{S^z\aj`adghkkloikrvwy{|~|}.Xe.[g.ir.is.wz.y|.{~.{..{..ev.i{.m~.m..n..w..w..z..z..... ..... .....,....4....."....I$DX..A..#6<8B.E.$D|.!....b<a..S&..,.,.$.K'GRZ..S&..fb...T.w`..(A..^H.*]...}...q!..X.jE....1.|.....Z.d..E..-..j."..-.....+.Z..n..T.C..Z..2Th. C..H...P..2..I9...0.....?_.4p...6r...G..9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Gotham-Black[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Gotham Black family
Category:	downloaded
Size (bytes):	69248
Entropy (8bit):	5.87377123134412
Encrypted:	false
SSDEEP:	768:mlorHqRAXoj1VDIyR3ae5EzMxI512oHW2dag8buKY5CIQm3WsD3yzrGJ9oflvs1b:nqbLIMprs8buTQmmsD30UisuUOb1klZ
MD5:	5F3D6E07DFEAE03CAA5E518FA46C28AD
SHA1:	10685F845D79193CBE78C572662EF56C02E5DE7C
SHA-256:	534B0A760F185A1F42250F91B54FF05B842CEE3AA3E796C3C6D8B7D3041D5E80
SHA-512:	69510348F35FF9F25A8B9B29FC361BEEA64CCDD120546B1A55BEBD9F7A72E380257C980D094C1E15798CECDEBEA873446A42C75F25430F25DEEDBA194D09E1F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/themes/custom/casella/fonts/Gotham-Black.eot?
Preview:	.....LP....[..@.....i.....G.o.t.h.a.m. .B.l.a.c.k.....R.e.g.u.l.a.r...".V.e.r.s.i.o.n. .2...2.0.0. .P.r.o.....G.o.t.h.a.m.-.B.l.a.c.k.....pFFTM^..... ...GDEF.o.....ZGPOS.n ....|..>"GSUB...`.....hOS/2Y.0....x...`cmap...G...x....gasp.....glyf.M.....$....head...c.....6hhea...E...4...$hmtxy.Ar.....loca).Q>...H....maxp.?.....X. .. name..6.....post*.....33..i._.<.....9.....9..... .8.....@.....2.....@..[.....H&FJ... ... .8..... ....M.....D.6..."....."....#....."...-.....9.....(...,.....).....p.!.m.....v.....).f...v.....+.&.1.&.....?...?...P.....>...'...>...>...>...'...>.G.C.4.....>.i.>.d.>...>.?.'...>.?.'... >.....6.....]....)...C.....*.X.....Y.W.....3.9.....^.....z.3.-.4.....[.3.-.8...3.z.3....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Helper[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 280x187, frames 3
Category:	downloaded
Size (bytes):	54394
Entropy (8bit):	7.956972919722851
Encrypted:	false
SSDEEP:	768:DSElKQvLQoTqFKJVYOYLhJNPFm97Nea2pS+I25oJfWv9cI/cdF5teT/FdJvVT7C1:DdvL9qk0PJNw97NQYtgifycd4DFbvtm1
MD5:	BE3F19FF565189F39708A4FAF877CB7C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Helper[1].jpg	
SHA1:	C730599FDAADC53E6E20074DFC03672332A0ED0B
SHA-256:	229B5F616F7199CA11C24C1B29E11B243DFE86CF04C3573A231DE82654D4CEEB
SHA-512:	F0957A3F6368184B74C736229C6212AE6C42353D6C9A3FD0603C4A663ADB81625722839A81BFB18F08B5FBE5B8902ADF635ED37F902F4F77818B946E01CDEDBA
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/Helper.jpeg?h=c775bc71&itok=yJ73e6-L
Preview:	.....JFIF.....`.`.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..#.-w.....M]7..y...K4Kkgg<K.YZ.!mV...7..-.8.`.1..../@.....M,R]K.7S#[...h...K"...y...#.. ....HP4..&..0...Z..~.....p.:f...W.T...\...---.Qj..\...r..g.....,-SN.....KV.....9%..K.....&"".R+yeh...X.f?.G9.+..,...a]\.6.n&Te...j.^.....m.....JQ.{.U/:r.I3....r...e..)...1P.c.8...e}z._....R7.,El..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\IMGL9024%20-%20worthingtonimages.com_RT[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 280x187, frames 3
Category:	downloaded
Size (bytes):	47496
Entropy (8bit):	7.948693765658309
Encrypted:	false
SSDEEP:	768:DTrF4NMGu3NYOGEzwa/QHu07Zpm3ZcIkIYwnFGt9+upri5R:D3FAMPJpz9/QdnomIGGcrif
MD5:	6E56A5969A359AD3C064D3AB02D19157
SHA1:	CCCD47A72F02AB53A89EE17EFD374EB24592F750
SHA-256:	DB0B4E03F7402D6E12D60D39445BFF1FEAB48B461C929A3F073A30164FA5BBEC
SHA-512:	30E64916304158CAB2164602DAC21F17684FC29F09F3002C393A243C976214FE2D7E1672383A00754B9EBB036787B56681512C0FEB1248F4FA16FC3C72EFB8B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/IMGL9024%20-%20worthingtonimages.com_RT.JPG?h=f2fcf546&itok=F_3T84nk
Preview:	.....JFIF.....`.`.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....b/*2F9.o.8.....q.q....WH..s.L.pjl.....R...A1IE$.V...<...3..d..Td..S.L[UIZU....7.....|....=?._.e.....q....W...u../.9#...wZ%g.&...T...H._....W.i.`s...s...r1.....!.d.....q...?O..#..u.....<s.{.5z.u.....<..9...+..rY.....q.....g..8.}.|.....{7...5m.....w.....g.8.2..I$..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\IR-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 204 x 152, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1704
Entropy (8bit):	7.050020806414554
Encrypted:	false
SSDEEP:	24:g1hfvWwjx82lY2T3iV8+yJ3VJVHG9Kftej5Quwg9zXGyJB8e9LL8:+ANn2eAJ3H9yAk9Iah9Lw
MD5:	F3803462C9A3BE12DCCC16D162F43733
SHA1:	9E766FC388882E50E48D912CFB65FEE3FD1384B6
SHA-256:	7F769844B6075B0FD7CC07F911AA40AFDFEEEDA44812058360CCA7B55F8EED64
SHA-512:	229C9BABEA01820A89CEDFBAA8C34FB5EFF7CD63CF57396B0BE611528032BD80E023CD70B3302A570E241E3B273F274062B01F14C8C0F36674C5F9915798BD9
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/i/misc/IR-icon.png
Preview:	.PNG.....IHDR.....=.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)" xmpMM:InstanceID="xmp.iid:4FF1FAAFDC6C11E6B58E9EFB08FEE97B" xmpMM:DocumentID="xmp.did:4FF1FAB0DC6C11E6B58E9EFB08FEE97B"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4FF1FAADDC6C11E6B58E9EFB08FEE97B" stRef:documentID="xmp.did:4FF1FAAEDC6C11E6B58E9EFB08FEE97B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....IDATx...?kSQ...D....~.....Zp.....ft.:..`.D..... b... ....$.bm!..M .....p=.y.....=....[.....:1...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JohnDoug-Truck_0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 480x384, frames 3
Category:	downloaded
Size (bytes):	117942
Entropy (8bit):	7.96808505540523
Encrypted:	false
SSDEEP:	3072:IC2BStqdDgVm9wwA24KF2mmbRR0ifTFkuma62PCjII6JjCG:x2stEDom/v2JR/62PCjI1
MD5:	B65E5FC080BBF23621D32A822FDDE6AE
SHA1:	DDE7005CC8906E9A04A14118D1992D8CA83DDA6C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\JohnDoug-Truck_0[1].jpg	
SHA-256:	3FBAE76374EFF7E9CE51D8A82F3142C0687588E813D7F740AFD49320A81743F3
SHA-512:	693B379A89E222D103CECB99675F901F4F09509304ECB94ED587046ACEB5244093BE9057077AFB4EB6264F79B83DD58C182D723EA64A491DAC61ADD2F2AE8D2
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/480x384/public/2016-12/JohnDoug-Truck_0.jpg?h=52a61b8e&itok=Q7rj68nk
Preview:	......JFIF.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..q...XK.....&mu.1.iR.xc....2...)e..Wz.i o.....F.....@T/.Ac..to%.A.k.....s_g\|,.~..C.C....^.>".....;...&%.'C.d..b$...A....w6b.u;]6....7.RX[...E.K+....k)... .0...Z.>rG.8X<..K.e...8-#.7W/h.I..c`.I..[...z.p.v..@..1o<.]...b.wg...0*p.t. .yTZZ...I....K.6....2)P..nM...w\.u.>..8..T.ym.L.1.....+.\m c...zE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Login[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 87a, 52 x 19
Category:	downloaded
Size (bytes):	1412
Entropy (8bit):	7.422177064958372
Encrypted:	false
SSDEEP:	24:IKjreoAX1BthLs+yQgt10S9sU6qqYCucdE58aOXfPVr4iHa:/uoAX1Bn4mgpyzx+YXVrvHa
MD5:	5027ABC5FCD8B396222C210C20201C4A
SHA1:	4D8DB48688A6E3F0FF063A899DD18995EAC0325D
SHA-256:	198A9CB339C89A12CF71AB5465CFDDD1A11AF223E260237F33202BCE7714B824
SHA-512:	6D91F13F832139E9F4417823DF3C2CD7BF758615C8DD58FF76C803911908E879BCF19806A1932C72520BD1029DF7AC16E492D385D3B2EFCE71E8EBC9FD5786B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure3.i-doxs.net/casella/images/Login.gif
Preview:	GIF87a4.....ZGKTGKUGKVFKYGL\KMSHN\HO_MPWRU[UWYGObKRcKSiW[eV[h]_aU^uR^{S^z\aj`adghkkloikrvwy{|~|}.Xe.[g.ir.is.wz.y|.{~.{..{..ev.i{.m~.m..n..w..w..z. .z..... .....|}.|}.|}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\PHOTO-LisaM[1].jpg	
SHA-512:	5927C5AB66E15CD1DB3FA082A98F180DAFFA12585D8B508A69C3C182F0B4B3C5DB23FA5E6431908AC3DFF7A6C90E347BCEE0C5ECBC7EB8DFFDE908FF5106D C98
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/PHOTO-LisaM.jpg?h=2992ba0a&itok=WlhPwy-4
Preview:	......JFIF.....`.`.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..|.9.K.....xw.P.n[.Ac..GP{A..m|.zu..<&f.(qj..C.....)....i.&i>3...u..x..C....+.u..i....B...]@....Y!.]:...|../.~*..Z...G.A..J...m.1i.x#V.|j....,R..1H.d.....!..>.(... .....S..:Rh.....t..M...c.....[<a.*1B....~.B..*..q2.V.H..iN....Z..WTi....~.N)*i.J..1.....)S.*.J.J..`..iB...7jr.:....i.V.\].....P..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\PayNow[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 87a, 62 x 19
Category:	downloaded
Size (bytes):	1616
Entropy (8bit):	7.487565611945328
Encrypted:	false
SSDEEP:	48:tGLrl1HPlO0eNeIS1FRu/w1lgxQUWt4TmXzDc/F:wR1H9Od01Fw4lgLXmXfc/F
MD5:	6F771A10C23070A0AF568106F44D88D0
SHA1:	1E945E2CEE57099AC06B1EC615EBE15188E68BF6
SHA-256:	DDBEA2C3A99694045CAADBAF31740814A914F995B6E3461D4541F1A1D53229FA
SHA-512:	79B3F7833C4231BFF1774237F8F3994868F343584A38F33329942C871929E7B6459A8FCBC4B021AA7BB427740311EEDDF2B5FA74AF8D4688FA0EF3A643C4FB32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure3.i-doxs.net/casella/images/PayNow.gif
Preview:	GIF87a>.....Z?BHFGIGHJFIMHIKIJKJKMHLVHMVJMTIMXIP_JP^NR\YZ\KQaLRaNVjQXiZ]cZ]fS[p^`b^`c_`c_ac_ad\an\e}`adfgjhikjlmklnoqtuvy\g.\g.bn.dq.w{.x|.y}.y~.z} .z~.s|.s}.m~.o..r..t..t..t..{..~.....~..... ....>.....Di.#E..+..8..a.....XHQ!.....H...-T.P"0...D...f.K6l.i.F..8.....9rt.3.f.jl..Ys..4SD...a..].f..K..Y.f.U..XY..+...Yc..... (N.....L....7h.x.*.0b...K...1..i...3.d.A...2d..H..v.re...#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Screen%20Shot%202020-09-23%20at%2011.40.28%20AM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	90493
Entropy (8bit):	**7.991382096398374**
Encrypted:	**true**
SSDEEP:	1536:7XCNJAsnNKqfsMpby5Q7iWzhwM1abQnhU6XqusFeDyG6CH3aBgSt8McOlhhPv:7X6nns4Ym7wM1pWhleWhCY381OSxv
MD5:	0434DB8079E4ECA815058D930209DC2F
SHA1:	4A5CFB254308FD5C596A0BB21BF6C035FF043B18
SHA-256:	0BCB0EC49242DD2F1A3E195115C36571FD1D21CC3EA40F5ECB6FE802899419F5
SHA-512:	0CABBD0693EA96D78794405B8D3C8C7DB874F0F3930E2C8419547BCAD370AEE41B7206F8355FC7CFFDA2EC0ED9C02FDECDD312334ACA0FDEE053F2FF1EA3 A5E
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/Screen%20Shot%202020-09-23%20at%2011.40.28%20AM.png?h=87ca5f37&itok=e674vuHm
Preview:	.PNG.....IHDR.....q.x....pHYs.....+.... .IDATx...K.n.v...U.....^.}.9.....m...%XD.v...$..A@...DB.A...4....XBB`.H"..8v...c;..s..}.~....Y5h.1.j....\|..k...Y.j....*.....5..DH9..R..k.H). ("r.....$....*..w..}..^.....;{.Ck"~_..xU{../.E..^...-.....r.r.&..2.L...^.....hU..&..N.%.zW.....b...i.....>....d..CQ....$:.N.B.O..8..z...$"..V..2gS&O.%-...:.I.. I.w.RUm>E(s..J.c'..V)U9.x./\.a..U.6..3xPa.g.... l.r.!1q..([..JAHl..v#.&..fL...(.VJ..T.sf_f.sa...,.S...)...ZQ...s.$..T.....0W(...Z.'T+3Pj..Bu.j.....b.k.V...$)!RA@H$.I.#..TF&.)^..0).!.7dxy. .....]>..P.I.?.q=..... &u,...?.T..`.`#6.M...v.r.rN.&...HR(..Jt..N.@2.YP)..Z.>tj.....c.p1....PC..v[;..9...j."l.Mk."l..R..Y..dML.r...m.....Z.d...$..Z..F1..*.(Z.U.O .N..`*..qu:[.LQ(A..$%.D.j}....iR&....a..... i.y.`-0.8.a.B.)s"J.ARb.....e....$J..[...*P....FM.T.&e.0....UH.U2.J..a.Z+..*BA...$..f..3.... .b...`.....r;.h....9....}.\....$..*.xg...5.\...e..7.#,.~....2..)."Z+...U+UaVE.1.bd.a.-...S.(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Screen%20Shot%202020-09-24%20at%2012.03.31%20PM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 280 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	108790
Entropy (8bit):	7.9883416699535035
Encrypted:	false
SSDEEP:	3072:BOTVXRewXx+i5oltihJSdvdnqts8spBtKmaYZX:BaVheix4ltiW1tZl
MD5:	5C86B1B86166D9F264FBF41D801D3301
SHA1:	2EAFE01D2AEF18E57D753C1383CABB898CDB7647
SHA-256:	4DFBD264280491FCFADC55A91C19359D6EF15C739F5DC35FF6AFB62C83C06BBD
SHA-512:	0040B1E16713EA0285D9B9A4362003E65CCCB6C7519AE044F3BBF6E698DC996CC767BA3B43AB25906AC602A2100BF2680E25197A033074151BE274DC64AACBB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Screen%20Shot%202020-09-24%20at%2012.03.31%20PM[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/280x187/public/2021-04/Screen%20Shot%202020-09-24%20at%2012.03.31%20PM.png?h=b6a95e15&itok=biC4NExs
Preview:	.PNG.....IHDR.....q.x....pHYs.....+.... .IDATx.t..l.u..[{8.DD.7.T.....(...@Y.n.B..~..1....`.....[....,-R...b.Uw.).s.....H:.....q.....}k....S...f..^_..#.2}.Y..B..X.....5.V.'... ...S..p.....q..k.X..0&.VLG.U...w.*.....7.....!.. q...q..Cp .3..X.T..Z).....>.*..J)L...O....?...K....'x..Q.|%,{.x..?...._ N...%.:.G.O.....k./q.....T.....[.n.|...,8:9.....g..h{..f..C.....iL..-..... .V...5.....}.Z.'.....8.l.4N.....;.p..9.....G...|.;....o1+d..R0._w..?....'...9.k>.....O.L..:su[(..^.{.x.A.....1....N.%.;F...6...,-.....:.j..B.G.n.Gpl...b.H%.a..> b...."NP...1.1.0..-..3.H@..... ...u..x..!....{T....@1...s.3#....].#..B`.X.bO..pO...."B....^..{D...3....90E....F.mm..Ua.FR..R....Z...K.....c..1.X..c..)%.....rJ.v;....0a.....o..._^..O.@I...'J.R.R.....SVKN. r...d.b<}...z.$z2.....j...7\m....\..>...BI'\\..qD.D0e.2.@..1:..U..!.p.6..!..a ....w...hf..{.1....V...s".... 8.l|~..@..k....l@..h..v.q.V...j...p.....G<..CV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Trailer%20dump_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 100", baseline, precision 8, 480x216, frames 3
Category:	dropped
Size (bytes):	39708
Entropy (8bit):	7.96202857940588
Encrypted:	false
SSDEEP:	768:nGhowggqqqahB7gF9pw5p0vuq4ajRY0aEFMx3APEFMYWuer+kC:nPwOqqwB7gF9a/ESatY0aD3APSerC
MD5:	7BDBE228F6D8A79D3FB3FD98CD81BA81
SHA1:	5B153FE57A17FA16EAA5C306E821106ACD7BFABF
SHA-256:	26B17B2AEC1FE2E3D1AC2A6B63EBE65EC77D9FED79FFC1CEF0A89DDF59A7DF60
SHA-512:	CDF6F74A005AE887685F021362879CE8E88DD5E2CA985BFB6D07FB0554751322881B1113E72C217100C3E2CCE0D210E7B3DE81316A3E41832272320637D0F6A5
Malicious:	false
Reputation:	low
Preview:	......JFIF.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....d.`x.'.zw.*E..5,Ssg...=8..O.].V.9.... .....8.....i1@....99q.X.w..}k.bX.....]o._~....:..-._..n..k..R.W. ....z.1.\.Nk[m.J...W.'...'.L.Q.S...c.e.p....R2s.... k6..)fa)#;G....;p....oJ.8.&...v}...?.....k_V.....4.2..\.....q..N..+2.L.W...P..$.A...;...ON9.E.F...i.....^9..ZZ..[....b.7n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Truck-business-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 75", baseline, precision 8, 1400x630, frames 3
Category:	downloaded
Size (bytes):	106422
Entropy (8bit):	7.951840271845407
Encrypted:	false
SSDEEP:	3072:GGVBxiVQi8PpOagtgbT/WQZxxyof2xGbzI0+EHDfWcbx5TJy69y:G2BxiVV8PpOagCbT/WQZx5k+fz5gn
MD5:	89FC8C3ED360DDBCC694FCE0217FC459
SHA1:	F4C36166824843DD53F4A28B9D6CBD7ABFD1672E
SHA-256:	2024C614EDBC071B8FB238B63AE98AFB8DC0BCB74E35E5A7BB92132126E4513E
SHA-512:	E6252A64F49A8A412E7D463045352F5C0BE8B3F454C26B3BFE002F7DFE8725EBC1843855EDFD38D6093B328DFEC0C0AB06D2F5C0AF5CB438B897F0E411F2EB3 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/styles/1400x630/public/2016-12/Truck-business-1.jpg?h=a7f9be62&itok=BWt-k-vt
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 75....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!22222222222 2222222222222222222222222222222222222222.....v.x.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTU VWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEF GHIJSTUVWXYZcdefghijstuvwxyz.....?..a..n;..|..N>tN.~4.....AH).....R.@.E.....`.....u.....GJ\Q.P.sK.....)h...iq..c..LQK.1.i. ....(...1E).Q.Z`%...P).....(....E..(..&(.-...{..i.....F)\..F94.(..Q.\R...U.7....ZwAF.(.)1N.8....QN..8.@...@.N.&(....4.b....9...}(.....Piz.\....1.QK.P.h....(....b..1.....:.^(..@..z\w..I..A.S....n:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\WMRT93B1.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	88108
Entropy (8bit):	5.255231125747819
Encrypted:	false
SSDEEP:	1536:RizltYqJr7yRNClGTjeLVAY7NeB+SIrWLgvDCgpSwovExT8uLxkh8DWBKtU3UvUm:RUqmeV86pVg5X60vviSEti50yH2Qz0sD
MD5:	8365F3AA02292375A4C400A63E480889
SHA1:	E5426BB4858E7C03E17DAC9B69759C33D6DAD4A6
SHA-256:	6D140534408A81DC513F83D8394AEC809E76557C777FF1C80BF4AC6A666993E7
SHA-512:	2302479925EAA2D159DF5214371B3A6472847276178494E40C0EE13D68836A51FF56A554DB3026D06B30526BFDDDE7E47E7D1970EF8FCCAF62A39F9D71833303
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\WMRT93B1.htm	
Preview:	<!DOCTYPE html>.<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# schema: http://schema.org/ sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http ://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema# " class="landing-page">. <head>. <meta name="google-site-verification" content="YDv Nl0VJhQJP6yrbLJp1-zQNGziQDoqCwwtXKBfJk2I" />. Google Tag Manager --><script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start': new Date().getTim e(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0], j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src= 'https://www.googletagmanager.com/gtm.js?id ='+i+dl;f.parentNode.insertBefore(j,f); })(window,document,'script','dataLayer','GTM-JSKKV');</script> End Google Tag Manager -->. <meta charset="utf-8" /><scri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\align.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	516
Entropy (8bit):	4.659087910408482
Encrypted:	false
SSDEEP:	12:U6dD/uKW9hFYaXTefgYe03jKqKCNILIEL9LyYBjfo/0V:3dil9T3DwgYL3jKvYPHo
MD5:	04D7490507FEC772BA9B77FF032847FA
SHA1:	E0A7D1EBC3D499FB65B42D4431237E15E273BCCB
SHA-256:	04A7A5360238B1BC854B61C4E04391B93141B57FE9266ECD3D5806D4E0353A82
SHA-512:	FFC5F098FE2982E760189ECE2F603F7DEDB3ECDFC9B801AC56C578D85BE00B8A9A8E2B57A8478EF5840B7F377C48DB5A5380856B8D23D8E3E634C65933774A 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/core/themes/stable/css/system/components/align.module.css?qljrib
Preview:	/**.. * @file.. * Alignment classes for text and block level elements... */.....text-align-left {.. text-align: left;..}...text-align-right {.. text-align: right;..}...text-align-center {.. text-al ign: center;..}...text-align-justify {.. text-align: justify;..}..../**.. * Alignment classes for block level elements (images, videos, blockquotes, etc.).. */...align-left {.. float: left ;..}...align-right {.. float: right;..}...align-center {.. display: block;.. margin-right: auto;.. margin-left: auto;..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\autocomplete-loading.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	633
Entropy (8bit):	4.944219293052727
Encrypted:	false
SSDEEP:	12:U6dMhiyFWH4dGfPRLMr5/AFilmb4M7uXHRLI3Vr5AN9mb4I3V7uXy:3daiykH4dmp+5/AoQb6Xxs5lbAXy
MD5:	2548D606F096D31AE1839C9E3331F37D
SHA1:	B9EBFF128AB3FB23C6D5F83F172418438177A49D
SHA-256:	24B16EAA0AF08A248F87ABDB33C3D90B858E02628ADA3C1CA366655CCC506374
SHA-512:	BAE0296F10C3E9D106D356DC2739D5070C0BD5C2EFF707069D57B3D82773DFEB642F9A1C9C64113E9CC72581B7175CD9E6589B9524FD93319ED6AA24311FE27
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/core/themes/stable/css/system/components/autocomplete-loading.module.css?qljrib
Preview:	/**.. * @file.. * Visual styles for animated throbber... *.. * @see autocomplete.js.. */.....js input.form-autocomplete {.. background-image: url(../../../images/core/throbber-ina ctive.png);.. background-repeat: no-repeat;.. background-position: 100% center; /* LTR */..}...js[dir="rtl"] input.form-autocomplete {.. background-position: 0% center ;..}...js input.form-autocomplete.ui-autocomplete-loading {.. background-image: url(../../../images/core/throbber-active.gif);.. background-position: 100% center; /* LTR */..}...js[dir="rtl"] input.form-autocomplete.ui-autocomplete-loading {.. background-position: 0% center;..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\capture[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	164155
Entropy (8bit):	5.434263098825111
Encrypted:	false
SSDEEP:	3072:b1SdOfcY+aBSIxjOBfwpw4Uc+hGpa5v3Ri7z5Xg:yOfia9KfwpwdV3iW
MD5:	6FD4624AC5413D01D355905086C7B1B5
SHA1:	F2E1A17285D08009D44440DE28C39B23C60BED31
SHA-256:	4DDD92DEC33C4103544854F91E46731612B8C288F0ABD7695230A08E01DCAC2C
SHA-512:	859C1538AB798A6159FA8FE03885C7D44416AFA5969E81AFFE0110F2F1C17DBC8B560CB10EE5CEA104C0D98ECD5C8DF74BC2E7EB25D6007E484913466902D5 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.rlets.com/capture_static/mms/capture.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\capture[1].js	
Preview:	!function capture(window,document,undefined){"use strict";if(window.RLCAP&&window.RLCAP.version)console&&console.warn&&console.warn("Capture has already been loaded.");else{var CAPTURE_VERSION="0698945cfd85ab10938f9864fdaae48b4d5e36dd";window.RLCAP=window.RLCAP||{},window.RLCAP.version=CAPTURE_VERSION;var hasInitialized=!1,CONSTANTS={CAMPAIGN_EVENT:"campaign_event",CONFIG_EVENT:"config_event",EU_VISITOR_CHECK_EVENT:"eu_visitor_check_event",OPT_OUT_CHECK_EVENT:"opt_out_check_event",SHOW_BANNER_EVENT:"show_banner",SHOW_IMPLIED_CONSENT_BANNER_EVENT:"show_implied_consent_banner",SIMPLIFI_EVENT:"simplifi_visitor_event",SIMPLIFI_INIT_EVENT:"simplifi_init_event",VISIT_EVENT:"visit_event"},BOTS={ahrefs:["AhrefsBot"],apple:["Applebot"],barracuda:["barracuda_vsm"],google:["Google"],yahoo:["Yahoo! Slurp"],yandex:["yandex.com/bots"],pingdom:["pingbot"],hubspot:["Hubspot Migration bot","Hubspot Webcrawler"],jobseeker:["JobBot"],leadcrunch:["CrunchBot"],opendi:["Opendi Screenshot Bot"],phantomjs:["S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\container-inline.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	235
Entropy (8bit):	4.48709628679562
Encrypted:	false
SSDEEP:	6:U6dqNT9rSTJu3WBQKO65MdeBlEfVvlHktF3jfo9:U6doTVM4a1O65eefERdktBjfo9
MD5:	134E3CD5110A796AA447C6E886D31B87
SHA1:	A3D77A34D43E600A6D4B025B3E31773DC70403B4
SHA-256:	49A31D020822A89EDA5B4FBE4D873BDD4BF94E66B6C9AFBA715B8279259EF79A
SHA-512:	31FE7B5E935C4CD26781BF2E01377A08540297D3004129A2A0A9516230DA71BA3AA57D5FFBA129259255B366052A7E09C9369E3A3704DC6804E8DDBD0794FFB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/core/themes/stable/css/system/components/container-inline.module.css?qljrib
Preview:	/**.. * @file.. * Inline items... */.....container-inline div,...container-inline label {.. display: inline;..}../* Details contents always need to be rendered as block. */...container-inline .details-wrapper {.. display: block;..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css__0ocaB9BRuNrmD5oFvZi50Nm5I9tkJRm0uksBslP4bY[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	48241
Entropy (8bit):	5.121831234225155
Encrypted:	false
SSDEEP:	384:GnliHUkTa0OPr2Zv5y3RRAxFnEf407g0XkJ/OUMAngMErHUapH6LpdxyFx1UpFbM:EkTa0OPr2Zv5yLilkUY6LnxyFMA
MD5:	8B2165D904525A5E6E5DB366700D3536
SHA1:	2DDC37F40D862C3B457E1B14200BB013A54A59E6
SHA-256:	FF4A1C681F4146E36B983E6816F662E74366E48F6D909466D2E92C06C94FE1B6
SHA-512:	2CFA3CD7C025B1A9C7CBC35841D796F04E722B7CF235C2F72DCFBDEA0530BA86DBF4E04207F4E205C38299AF677C2064324C30CF1255A090E38C85EFCB59539
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ir.casella.com/sites/g/files/knoqqb53536/files/css/css__0ocaB9BRuNrmD5oFvZi50Nm5I9tkJRm0uksBslP4bY.css
Preview:	[ndq-data-icon]:before{font-family:"ndqfonticons" !important;content:attr(ndq-data-icon);font-style:normal !important;font-weight:normal !important;font-variant:normal !important;text-transform:none !important;text-decoration:none !important;display:inline-block;speak:none;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;font-size:30px;vertical-align:bottom;padding-right:5px;}[class^="ndqicon-"]:before,[class*=" ndqicon-"]:before{font-family:"ndqfonticons" !important;font-style:normal !important;font-weight:normal !important;font-variant:normal !important;text-decoration:none !important;display:inline-block;text-transform:none !important;speak:none;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale;font-size:22px;vertical-align:middle;}.ndq-icon svg{fill:#000}.ndqicon-briefcase-1:before{content:"\e068";}.ndqicon-briefcase-2:before{content:"\e069";color:#454545;}.ndqicon-briefcase:before{content:"\e02a";color:#454545;}.nd

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\custom[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37438
Entropy (8bit):	5.3548670809167245
Encrypted:	false
SSDEEP:	768:9J1HrtZnLuZnW9ZnG4R4fn8tfJSX0eAshCFGFeFqLETPhG:/xrtZnLuZnW9ZnWn8yX0eAshCIEDTPhG
MD5:	386A1EDC686C5509CD2E75335492111D
SHA1:	2E7AD27C47759E3B975092954BC585860B3CEA87
SHA-256:	D1BE550FA641EA4EA543F9B52111B3CF9A0508601FEB1C102D618E8D92559205
SHA-512:	31D89993EFE9BCB7ADE0A083C7C53F1E1D1843586970AAED3FCF14134AE0E0B689AE5FBE18464F6409CAC9E0D4A7384D727986F3C823BEC1922F6EEF0D4D46CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/css/custom/custom.css?qpcosx

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\custom[1].css	
Preview:	/*.Website Name: High Peaks Resort.Description: Global/General stylesheet.Version: 1.0.Author: Adworkshop.Author URI: http://www.adworkshop.com.*/../* ========== == */./* FONTS */./* ================================== ========== */. @font-face {..font-family: 'Gotham-Black';..src: url('../../fonts/Gotham-Black.eot');..src: url('../../fonts/Gotham-Black.eot?#iefix') format('embedded-opentype'),...url('../../fonts/Gotham-Black.woff2') format('woff2'),...url('../../fonts/Gotham-Black.woff') format('woff'),...url('../../fonts/Gotham-Black.ttf') format('truetype'),...url('../../fonts/Gotham-Black.svg#Gotham-Black') format('svg');..font-weight: normal;..font-style: normal;.}..@font-face {..font-family: 'Gotham-Bold';..src: url('../../fonts/Gotham-Bold.eot');..src: url('../../fonts/Gotham-Bold.eot?#iefix') format('embedded-opentype'),...url('../../fonts/Gotham-Bold.woff2') format('woff2'),...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\custom[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	38194
Entropy (8bit):	5.3898171455076955
Encrypted:	false
SSDEEP:	768:lJ2wqJSI/40u4q4ucTLfKwvAP+hBI9eV6rex:HpqcKPycTVDhT6rex
MD5:	AA3D526C4BA3A1A7E8F2F90095BA1AB3
SHA1:	C2D13C71757624E19466D49F07105973E14DAAB1
SHA-256:	8D37EF96CF3EC7AF5EF8470831B0D895D049264836F703B68BF90D86042B466F
SHA-512:	DF6C1480301D645582A9526699037557A409D203A88008D9012507353E8A348257CA0E80A1B39FB9AE3C8C435108B46E2C10C55C0B0817775694683F5CE745E3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/themes/custom/casella/css/custom/custom.css?qljrib
Preview:	/*..Website Name: High Peaks Resort..Description: Global/General stylesheet..Version: 1.0..Author: Adworkshop..Author URI: http://www.adworkshop.com..*/..../* = ========== == */../* FONTS */../* ========== ========== */.. @font-face {...font-family: 'Gotham-Black';...src: url('../../fonts/Gotham-Black.eot');...src: url('../../fonts/Gotham-Black.eot?#iefix') format('embedded-opentype'),....url('../../fonts/Gotham-Black.woff2') format('woff2'),....url('../../fonts/Gotham-Black.woff') format('woff'),....url('../../fonts/Gotham-Black.ttf') format('truetype'),....url('../../fonts/Gotham-Black.svg#Gotham-Black') format('svg');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'Gotham-Bold';...src: url('../../fonts/Gotham-Bold.eot');...src: url('../../fonts/Gotham-Bold.eot?#iefix') format('embedded-opentype'),....url('../../fonts/Gotham-Bold.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dest5[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6983
Entropy (8bit):	5.483922930498494
Encrypted:	false
SSDEEP:	96:inw1EOb9muLpw47eIDCpXHG5z/QkqJeMnSSyi8c2Kgn/UnNsnA2al4j4e:iPc/xDCpX8/in/y+2KgMSA26l
MD5:	2C9C2EE145EE280B85A217AD7045FAE5
SHA1:	6ABE394B53B32816ECA642126FD62BCD91D17348
SHA-256:	7BEA17A80A61ED0F54248B4FFC4C718F7C8FF2619742577A73591D62CE074DA8
SHA-512:	3762C5F678EB4858000FCF379EA1C8BEA54F2A211A3F940300876D1697B82012C57B0E614E33770D8F5626B2F4C3B7842B658C926E12974A43A1B0A313E2DB79
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">.<html lang="en-US"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><title>Adobe AudienceManager</title><script type="text/javascript">.var Demdex={version:"6.2",dest:"5",PROTOCOL:"https:"==document.location.protocol?"https:":"http:",COOKIE_DOMAIN:function(){var a=document.domain;/demdex\.net$/i.test(a)&&(a=".demdex.net");return a}(),SIX_MONTHS_IN_MINUTES:259200,THREAD_YIELDING_DELAY:100,errorReportingEnabled:!1,sent:[],errored:[],timesDextpWasCleared:0,dpids:null,cbmacros:["%timestamp%","%rnd%","%did%","%http_proto%"],validators:{isPopulatedString:function(a){return"string"==typeof a&&a.length}},addListener:function(){if(document.addEventListener)return function(a,.b,c){a.addEventListener(b,function(a){"function"==typeof c&&c(a)},!1)};if(document.attachEvent)return function(a,b,c){a.attachEvent("on"+b,function(a){"function"==typeof c&&c(a)})}}(),replaceMacro:f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\embed[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	39819
Entropy (8bit):	5.240122704158427
Encrypted:	false
SSDEEP:	768:z2aA6BVRJ/LGhSOFjwpVtcSOmRVy+GV2UKDLo459fk9qwMILi9MS/v/FZVeG/GfX:i6BVRJ/LhVy+21KD359fk9qFILi9N/do
MD5:	C913338EECFA5E495053A7FFD9EE7E40
SHA1:	B606F5C84AA375116D1626D036983E4F76DA6FF7
SHA-256:	F4F7FA29F3661A499112FE623C00887924A2456D5847BE5BBBA2E60F77978F8F
SHA-512:	4CEA784953BE82CF95B2364D3DE4A8D12FFD0D14EB639BD34DD52C8398E54042938AA664EA138A69CFD8D375EBBA26EE6D0BE2644B5CE5759BE431C78279253
Malicious:	false
Reputation:	low
IE Cache URL:	http://apps.twinesocial.com/embed?app=casella&layout=251053&showLoadMore=yes&autoload=no

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\embed[1].js	
Preview:	if (typeof TwineSDK == 'undefined') {...Twine = {}; // global object container..Twine.frameArray = new Array();...var TwineSDK = {....// default to autoLoad the hub; set to false to manually load...autoLoad: true,....// default settings for networks...// an example:...networks: {},....// load the Twine hub using this specific tab id...// it sends it to the first twine iframe on the page...// no way to send it into a second iframe on the page...// we could send in a parameter if it is a problem...LoadTabById: function (tabId) {....document.getElementById('twine-iframe-' + Twine.frameArray[0].instanceId).contentWindow.postMessage(JSON.stringify({verb: "load-tab",data: tabId}), "*");...},....setIFrameSrc: function(nurl,iFrameID) {....if (!document.getElementById(iFrameID).src) {.....document.getElementById(iFrameID).src = nurl;....}...},....executeCTAEvent: function(el) {....var action = jQuery(el).attr('data-cta-action'),.....cta_id = jQuery(el).attr('data-cta-id'),.....media_id = jQue

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36606
Entropy (8bit):	5.497235992375013
Encrypted:	false
SSDEEP:	384:K49S+7D2RCcqbzAGfn292c3Lxa6l5rDcJcRAeYUAkP/e5KNCsNSDAhcjCSJ1pOu1:7B7jciAat4JGYUAkXusAjebvm48XoU
MD5:	645EE2F03A1C6F1C98B0A1E0A7DB00DA
SHA1:	F93FE04BB5D2E3A1AA7446A4125ED2F9A9BB5BAD
SHA-256:	C322060C87967C74E8E1469862CAB247AD7AA0C66E35918333904A125EDCF3B3
SHA-512:	2A1D418C15B101AA028F89F176ABD5FEDC21BE38E70D0CD9BC530F593585DCA0A34E4C77AED2A8B8350B5B92509D22F115E7F39828837CF9FF945AE4127EE15F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),l={},fa={};function p(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function v(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in l?f=l:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:null;b=b(c)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fa0a609357[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.254849015882737
Encrypted:	false
SSDEEP:	3:U3KTDWTwTWMWVrfVh:HAFMWVrn
MD5:	5C9DA71976FB9D00F82E61C7E496BA06
SHA1:	58884FB0E24A399213205AD35DB27E6011BD149C
SHA-256:	F69A13217482DC43F25E74CFCB9391D0F06D22501F10F5CB5E413D2D98A5CD23
SHA-512:	DBC11417F6342430D30220B7A4F141F05801520C429CC1C80FEC974BA840AF1D4C316395CF9B12AAFBC36F04795A0558BEAEC690D43C31FBB86175C2B41557E
Malicious:	false
Reputation:	low
Preview:	NREUM.setToken({'stn':0,'err':0,'ins':0,'cap':0,'spa':0})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fa0a609357[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.254849015882737
Encrypted:	false
SSDEEP:	3:U3KTDWTwTWMWVrfVh:HAFMWVrn
MD5:	5C9DA71976FB9D00F82E61C7E496BA06
SHA1:	58884FB0E24A399213205AD35DB27E6011BD149C
SHA-256:	F69A13217482DC43F25E74CFCB9391D0F06D22501F10F5CB5E413D2D98A5CD23
SHA-512:	DBC11417F6342430D30220B7A4F141F05801520C429CC1C80FEC974BA840AF1D4C316395CF9B12AAFBC36F04795A0558BEAEC690D43C31FBB86175C2B41557E
Malicious:	false
Reputation:	low
Preview:	NREUM.setToken({'stn':0,'err':0,'ins':0,'cap':0,'spa':0})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fa0a609357[3].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fa0a609357[3].js	
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.254849015882737
Encrypted:	false
SSDEEP:	3:U3KTDWTwTWMWVrfVh:HAFMWVrn
MD5:	5C9DA71976FB9D00F82E61C7E496BA06
SHA1:	58884FB0E24A399213205AD35DB27E6011BD149C
SHA-256:	F69A13217482DC43F25E74CFCB9391D0F06D22501F10F5CB5E413D2D98A5CD23
SHA-512:	DBC11417F6342430D30220B7A4F141F05801520C429CC1C80FEC974BA840AF1D4C316395CF9B12AAFBC36F04795A0558BEAEC690D43C31FBB86175C2B41557E
Malicious:	false
Reputation:	low
Preview:	NREUM.setToken({'stn':0,'err':0,'ins':0,'cap':0,'spa':0})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	813
Entropy (8bit):	7.058318274293224
Encrypted:	false
SSDEEP:	24:hXeUfKO+xZ61+0dayZ4ua66zjW6EMCppvKEfl9:hV+xoPZ4uEG6EVppNT
MD5:	6258DFE671D9CF189232A625569C67B6
SHA1:	C7EF886735BFABCB4AE10B4249D9E750A70E7EDB
SHA-256:	AF10AAFD29541ED5308241E60675D7B6737F6D380E4D0DB6B81B1FEC9FC5E551
SHA-512:	6572DB41C848F0AB7F3239EC5C6677B39C8A06F11EA87229B04D654236BB62A2E8B4D2E93A6DC6F2FB3B1CBF7D2F488DC71D1C49FF547F2DB3AFD8A75E6F2FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/i/favicons/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .D.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....PLTE.+Ap.....8M...Xq..&>.....Idt.9N:Wj....2G.+B.....?S/N`(H\.1F.8M.8M.8M.:O.:O.<P.<P.=R.>R.<Q.....'=.....&=:Xi.....Yq.....'>.+Ax.....Nhx.&=.&=....6.{...9tRNS.....bKGD:N.....pHYs.....L"M.....tIME.....0.....IDAT8.c.$.....+`fa.(`....A.8p.[q.R.E...<.|.....=&(.[.08lD.).%.@L..$.+@..L..R.2.r...J.....W...R..[.....V:.zVx.....)0.'ZC..F.`.&.f.....~...n.0.O.....%tEXtdate:create.2017-01-03T16:48:18+01:008.qd...%tEXtdate:modify.2017-01-03T16:48:18+01:00I.....tEXtSoftware.www.inkscape.org..<....WzTXtRaw profile type iptc..x.....qV((.O..I.R..#..c..#.K....D.4.d.#.T .....H.J.....t.B5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon-32x32[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	813
Entropy (8bit):	7.058318274293224
Encrypted:	false
SSDEEP:	24:hXeUfKO+xZ61+0dayZ4ua66zjW6EMCppvKEfl9:hV+xoPZ4uEG6EVppNT
MD5:	6258DFE671D9CF189232A625569C67B6
SHA1:	C7EF886735BFABCB4AE10B4249D9E750A70E7EDB
SHA-256:	AF10AAFD29541ED5308241E60675D7B6737F6D380E4D0DB6B81B1FEC9FC5E551
SHA-512:	6572DB41C848F0AB7F3239EC5C6677B39C8A06F11EA87229B04D654236BB62A2E8B4D2E93A6DC6F2FB3B1CBF7D2F488DC71D1C49FF547F2DB3AFD8A75E6F2FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ir.casella.com/sites/g/files/knoqqb53536/files/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .D.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....PLTE.+Ap.....8M...Xq..&>.....Idt.9N:Wj....2G.+B.....?S/N`(H\.1F.8M.8M.8M.:O.:O.<P.<P.=R.>R.<Q.....'=.....&=:Xi.....Yq.....'>.+Ax.....Nhx.&=.&=....6.{...9tRNS.....bKGD:N.....pHYs.....L"M.....tIME.....0.....IDAT8.c.$.....+`fa.(`....A.8p.[q.R.E...<.|.....=&(.[.08lD.).%.@L..$.+@..L..R.2.r...J.....W...R..[.....V:.zVx.....)0.'ZC..F.`.&.f.....~...n.0.O.....%tEXtdate:create.2017-01-03T16:48:18+01:008.qd...%tEXtdate:modify.2017-01-03T16:48:18+01:00I.....tEXtSoftware.www.inkscape.org..<....WzTXtRaw profile type iptc..x.....qV((.O..I.R..#..c..#.K....D.4.d.#.T .....H.J.....t.B5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93774
Entropy (8bit):	5.392602416896564
Encrypted:	false
SSDEEP:	1536:sM+OWt6w6aic9MeipKKqQqcThe7Kdv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiX:sOQMj1SVBYDGKx

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fbevents[1].js	
MD5:	077B8B6E85C9EDF74D372D155180E6D3
SHA1:	4A24BE343819AD355807ADB01579366A1E64B8B9
SHA-256:	A517525B8A7D39BCAF1CF5F9695C5BE8FCE7A6B920A3924C1A4F70E8EA748C05
SHA-512:	DB714A2EAF14E6727086795FE151F3729DA32BFA0B87AB74289B7DF9E0808E1FEBCA38D2622EF47B7AA263479BDB66857011E2302DD1AFC9E814EF6B74642DF9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fieldgroup.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	104
Entropy (8bit):	4.461978028205114
Encrypted:	false
SSDEEP:	3:U6dDeZWKQNVQWAtWPKyoPBPTQ/HuB62nfF0Jrnt:U6dqZC/QWyWPKycPc/HO/Fsh
MD5:	06380BC2E356228B2062789C877F97EE
SHA1:	C45B4C44207982AD34A740002E579F3ADE45804C
SHA-256:	833B0D5C6E389060D934CC3904FD64D9BB35354229758B6804C913587BAAB583
SHA-512:	C84D1479A7CAE160860FDA630365A32AB65B3129E901DD4D8317A234F5C1D9AA80C3E652E21F6CF75A97AA461481824EEED4EE95157EEEE8813B9EF8DC42A2C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/core/themes/stable/css/system/components/fieldgroup.module.css?qljrib
Preview:	/**.. * @file.. * Fieldgroup border reset... */.....fieldgroup {.. padding: 0;.. border-width: 0;..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29063
Entropy (8bit):	4.755267089852831
Encrypted:	false
SSDEEP:	384:Uu5yWeTUKW+KlkJ5de2UYDyVfwYUas8l8yQ/8dwwdG:flr+Klk3Yi+fwYUf8l8yQ/eC
MD5:	4083F5D376EB849A458CC790B53BA080
SHA1:	FB5B49426DEE7F1508500E698D1B3C6B04C8FCCE
SHA-256:	008A1D103902F15FDB1C191FCB1CE8954330E7B8DE43D09ABB08555BA609F420
SHA-512:	E2E1991E96C3962371880BFF43364DA3FC9BD85B405FEAA20DBEF2A415A211D2505FC3EE829F0CEA297949190DF2342B0CB5AC877AEB3C349745FDC3C0560CDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/plugins/font-awesome-v.4.6.3/css/font-awesome.min.css?qpcosx
Preview:	/*!. * Font Awesome 4.6.3 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.6.3');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.6.3') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.6.3') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.6.3') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.6.3') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.6.3#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fullWidthPromo2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1440x900, frames 3
Category:	downloaded
Size (bytes):	201924
Entropy (8bit):	7.973356171783263
Encrypted:	false
SSDEEP:	6144:ucXIoumsSD//WclQGqdnhdxIWPrNz6/KW53W:ZYoulQ/mrdxIWVUK
MD5:	8C47E8D8B024C2975968FFCE70E571F2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\fullWidthPromo2[1].jpg	
SHA1:	21914099CFFD308726135AAD30318C44F57D2C58
SHA-256:	7EC0DEE54A758C2FE7C305DC90CDE1624B664E3D602EB55A46F0C912C461C54B
SHA-512:	9C8F88192B088E9298FF49C17FA30DD99EE625F125ACEA636C13186009A848E220A85988F9970390F47C999759C6123019BC9FE7A3E062B6C73E6479748933DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/sites/default/files/2016-11/fullWidthPromo2.jpg
Preview:	......Exif..II*.....Ducky.....2.....3http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:200A195F453011E6AA3DC438A8F8E659" xmpMM:InstanceID="xmp.iid:200A195E453011E6AA3DC438A8F8E659" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:AD4D9278412411E6BBDFA7B2533248F2" stRef:documentID="xmp.did:AD4D9279412411E6BBDFA7B2533248F2"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....#"""#""""".....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	80399
Entropy (8bit):	5.517175005595233
Encrypted:	false
SSDEEP:	1536:7b0NdVQ0i+H7wuo6Ni7QSN27sDjd0rrNSt81z9jKPfmTJ0NSoiUT:7b0Ns0Y4ABjOrNStkoiUT
MD5:	F3A67CD3CF1BFE48812ECDBEB369B057
SHA1:	1CF5C9047A18BF92BE584AA023B637B3F9B1A57F
SHA-256:	D7775ECD3DE7541926A952EF7F189FB1DF1B69F2005DCE942AD8B9F1CB1D431F
SHA-512:	0F4E299E62D11AEE673D6E5FA06A7B809C0E94FE4502E607CD083496409451849BCC28F9F5481F93F51D4A5EB72471BF9F34EA89DD89300D2706EAAC8F56025A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-N966XSH
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__c",. "vtp_value":"UA-5572590-5". },{. "function":"__u",. "vtp_component":"URL". },{. "function":"__u",. "vtp_component":"HOST". },{. "function":"__u",. "vtp_component":"PATH". },{. "function":"__f",. "vtp_component":"URL". },{. "function":"__e". }],. "tags":[{. "function":"__ua",. "once_per_event":true,. "vtp_overrideGaSettings":true,. "vtp_trackType":"TRACK_PAGEVIEW",. "vtp_trackingId":["macro",1],. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false,. "vtp_enableFirebaseCampaignData":true,. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]].},."runtime":[].....};../*.. Copyright The

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4029
Entropy (8bit):	5.214303610589507
Encrypted:	false
SSDEEP:	48:CB2LDddN8XZ+VZuTBx6Y9aJFTDtN4QELLDa8Bx6YCVZViwsBd3rOOfrlQ8FijSbg:NN4ZGAT29P8arh8QZ
MD5:	69EB8C34CB9FEA182EA40CE74E9FFC9A
SHA1:	2155612E5A3182EB0B945E1BC09CB49DBEB92D98
SHA-256:	B36ACE30B58B88931BE593FEA0B54876434CED7493967798C136DFEE98A12644
SHA-512:	E4D2A0D88433D577A8560FD11697188BF0C596A8A9DD51E2C7F1B7D18E3A63B614A1D94C0592E3A7C77A4797DD6E81E6CD15F077851C6E109292FF11F1F1844
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/js/custom/home.min.js?v=1.x
Preview:	function equalheight(e){var r,i=0,o=0,n=new Array;jQuery(e).each(function(){if(r=jQuery(this),jQuery(r).height("auto"),topPostion=r.position().top,o!=topPostion){for(currentDiv=0;currentDiv<n.length;currentDiv++)n[currentDiv].height(i);n.length=0,o=topPostion,i=r.height(),n.push(r)}else n.push(r),i=i<r.height()?r.height():i;for(currentDiv=0;currentDiv<n.length;currentDiv++)n[currentDiv].height(i)})}window.addEventListener("DOMContentLoaded",function(){"use strict";jQuery(".accordion-toggle").on("click",function(e){e.preventDefault();var r=jQuery(this),i=r.next(".accordion-content"),o=jQuery(this).children(".toggle-icon"),n=jQuery(this).parent(".accordion-container");r.toggleClass("open"),i.slideToggle(250),r.hasClass("open")?(o.html(""),n.addClass("selected")):(o.html(""),n.removeClass("selected"))});var e=jQuery("#home-slider").html();function r(e){var r=Modernizr.mq("(min-width: 1200px)"),n=jQuery("#home-slider").dat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	22334
Entropy (8bit):	5.06890079606409
Encrypted:	false
SSDEEP:	384:OsFNvT6hZFU3SKaMPU6gcmTPFGFeFkFmFGFeF4TxC2Ar:RFNvT6vFU3SKaMPU6gcqPFGFeFkFmFGO
MD5:	21553BF166F52A4E1F96FEC668203C3B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\home[1].css	
SHA1:	DFCEB08F63846FA15D36DABA8B9D5668D0DB2691
SHA-256:	2D63B4F96E3BF93B7933ADD1CFFAA6A26D825D154F3C200F5D64EF5C6DA6221C
SHA-512:	F6435277AF954932D356E72A5625C53E695E9EE74C64F944BEF761004327512945347E32500A2E1C0865156F76DDA88A5075F593B17402FD98E4D96957C6E692
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/css/custom/home.css?qpcosx
Preview:	/*.Website Name: Casella.Description: Home Page specific stylesheet.Version: 1.0.Author: Adworkshop.Author URI: http://www.adworkshop.com.*/../* ========== ========== */./* HEAD/UPPER REGION */./* ========== ========== */ . .home-headerPanel-container {background:#0a253e; width:100%; padding:60px 0; text-align:left;}. .home-headerPanel-container h1 {color:#FFF; font-size:40px; text-transform:uppercase;}. .home-headerPanel-container h1 span.white {color:#FFF;}. .home-headerPanel-listContainer {margin:20px 0 0; line-height: 1.5;}. .home-headerPanel-listContainer:before {content:''; display:block; width:80px; height:1px; border-top:1px solid #265736; margin:25px 0 20px;}. .home-headerPanel-listContainer ul li {display:block;}. .home-headerPanel-listContainer ul li:before {content:'\2022'; display:inline-block; color:#fff; margin:0 10px 0 0;}. .home-headerPanel-listContainer ul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ibs_dpid=269&dpuuid=cc3a6091-a4b5-4a00-95ec-94d4d16e385b[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\iframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12291
Entropy (8bit):	5.478244112341409
Encrypted:	false
SSDEEP:	192:6BNKHoBIyOTP0TE9RJp/CipesEdBS1wTQXK2BEtyOTP0T1U2Jp1YipesEdBS1wT8:6BNKIBW08JHUoK2Bc0bJPUe
MD5:	4E694592ADB84FFBA79A0F6E283BC767
SHA1:	D4874AF094D9D7D5B6E948B0297D279BAEF00AD2
SHA-256:	D8E37AC241343558A12AE83AAF3AB693F29F24B59ECD088CFF37329B12B833B5
SHA-512:	A96DE1C83F3BB0B725343B3FD3459ECC32470F864234DC11ABD94D4BA401C9D7143193F3D5B68DEF7A07BED0C2FC12050330FBBF7915899A7A376411C7BAC6 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.mathtag.com/sync/iframe?mt_uuid=b1b55f46-7936-4001-9dfc-67a6a8fcc405&no_iframe=1&mt_adid=187218&source=mathtag
Preview:	<html><body>.<script type="text/javascript">.try {. /**/.(function() {. try {..var sync_4815162342 = function() {.this.urls = [.[0, "https://pixel.mathtag.com/misc/img?mop_seq=0:28&mt_cb=835433&mop_top="],.[9, "https://pixel.rubiconproject.com/tap.php?v=4222&nid=1512&put=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&expires=28"],.[4, "https://cm.g.doubleclick.net/pixel?google_nid=mediamath&google_cm&google_hm=zDpgkaS1SgCV7JTU0W44Ww"],.[13, "https://ib.adnxs.com/getuid?https://sync.mathtag.com/sync/img?mt_exid=13&mt_mminit=1&mt_exuid=$UID"],.[3, "https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTM2MiZ0bD00MzIwMA==&piggybackCookie=uid:cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[5, "https://eu-u.openx.net/w/1.0/sd?id=536872786&val=cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[15, "https://dsum-sec.casalemedia.com/rum?cm_dsp_id=3&external_user_id=cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[21, "https://pixel.advertising.com/ups/55938/sync?uid=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&_orig

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\iframe[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6207
Entropy (8bit):	5.4890276806147655
Encrypted:	false
SSDEEP:	192:hK2BEjZuyOTP0T19Zyy6Jpy3ZyySipesEdBS1wTQMFk:hK2Bn00JOUq
MD5:	74279C91E120111F208D880C23CB57EE
SHA1:	DC3F346B14BBC80E8C4C3861C955CD7423A52DE8
SHA-256:	8E6E1209A98BEC8AAD8595E8CFB09E6244D4A91D0A863384A6720F9EBB671831

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\iframe[2].htm	
SHA-512:	A7858F5BBD6DE45BA13AE5947BEA43B75230B5913863F95C548BD68DE8A3C5BD4207F877B5EDC51DE1AE4F01E4E899F32BFF111BEA115405A38FDDB94D4D81AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.mathtag.com/sync/iframe?mt_uuid=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&no_iframe=1&mt_adid=187218&source=mathtag
Preview:	<html><body>.<script type="text/javascript">.try {. /**/.(function() {. try {..var sync_4815162342 = function() {.this.urls = [.[0, "https://pixel.mathtag.com/misc/img?mop_seq=0:28&mt_cb=229175&mop_top="],.[9, "https://pixel.rubiconproject.com/tap.php?v=4222&nid=1512&put=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&expires=28"],.[13, "https://ib.adnxs.com/getuid?https://sync.mathtag.com/sync/img?mt_exid=13&mt_mminit=1&mt_exuid=$UID"],.[3, "https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTM2MiZ0bD00MzIwMA==&piggybackCookie=uid:cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[5, "https://eu-u.openx.net/w/1.0/sd?id=536872786&val=cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[15, "https://dsum-sec.casalemedia.com/rum?cm_dsp_id=3&external_user_id=cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[21, "https://pixel.advertising.com/ups/55938/sync?uid=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&_origin=1"],.[10010, "https://stags.bluekai.com/site/4448?id=cc3a6091-a4b5-4a00-95ec-94d4d16e385b"],.[46, "https

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21EFDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.mathtag.com/misc/img?mop_seq=0:28&mt_cb=229175&mop_top=
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21EFDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sync.mathtag.com/sync/img?mt_exid=13&mt_mminit=1&mt_exuid=5955513615460275225
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[3].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21EFDC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[3].gif	
IE Cache URL:	http://https://pixel.mathtag.com/misc/img?mop_seq=20:28&mt_cb=232790&mop_top=9:1620155996|13:1620155996|3:1620155996|5:1620155996|15:1620155996|21:1620155996|10010:1620155996|46:16201559 10017:1620155996|10074:1620155996|10072:1620155996|42:1620155996|44:1620155996|17:1620155996|39:1620155996|10041:1620155996|30:1620155996|10092:162 55996|10008:1620155996|26:1620155996|
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[4].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21E FDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.mathtag.com/misc/img?mop_seq=28:28&mt_cb=771320&check=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&mop_top=9:1620157641|13:1620157641|3:1620157641|5:1620157641|15:1620157641|21:1620157641|10010:1620157641|46:1620157641|10017:162015 1|10074:1620157641|10072:1620157641|42:1620157641|44:1620157641|17:1620157641|39:1620157641|10041:1620157641|30:1620157641|10092:1620157641|10008:1 157641|26:1620157641|50:1620157641|10025:1620157641|10031:1620157641|36:1620157641|10040:1620157641|10004:1620157641|10009:1620157641|10089:162015 1|
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[5].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21E FDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pixel.mathtag.com/sync/img/?mt_exid=10009&mt_exuid=
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[6].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21E FDC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\img[6].gif	
IE Cache URL:	http://https://pixel.mathtag.com/misc/img?mop_seq=28:28&mt_cb=913507&check=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&mop_top=9:1620155996|13:1620155996|3:1620155996|5:1620155996|15:1620155996|21:1620155996|10010:1620155996|46:1620155996|10017:1620155996|10074:1620155996|10072:1620155996|42:1620155996|44:1620155996|17:1620155996|39:1620155996|10041:1620155996|30:1620155996|10092:1620155996|10008:1620155996|26:1620155996|50:1620155996|10025:1620155996|10031:1620155996|36:1620155996|10040:1620155996|10004:1620155996|10009:1620155996|10089:1620155996|&final&timings=0:166|9:251|13:254|3:9|15:9|10074:9|5:113|10004:109|42:180|39:180|0:180|0:186|10072:248|44:255|10010:262|0:266|10092:278|30:289|26:292|50:350|10040:476|46:603|10009:696|36:1214|10041:1960|&errors=21:182|10008:248|10031:320|10017:381|10025:444|17:656|10089:1385|
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4598
Entropy (8bit):	5.274424813815875
Encrypted:	false
SSDEEP:	96:Qty8grfp3fGfpNJutdJWfbQdXwe5B8hKXWosbVZoprghFOuvrNCj:QaGbQd5PKvw
MD5:	33ED216EF4569E95A97E55FB39D91D38
SHA1:	9849B887B9D36E35355DFEC4EA142AC455CF9190
SHA-256:	41F1E9970B646AADAC0F40543BB08B21E49990BF1B09392D1EF4D71B275069EA
SHA-512:	0F083D5F8DB6D5A49424C3E10947A387416BA57DB6279E2AFC2ECB8763AED3531FBA8DE0155B3CDAB9578E878E51D51C527AC97F60C6F5DC120FAFD257AA754
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.adroll.com/j/pre/5GUGQOHJCNCCRMXAOQX6O6/44LNCGAYPJDXFK7VEUPB5B/index.js
Preview:	(function(m){(function(c){function l(a){return null===a||void 0===a?a:!!a}function y(a,b){if(!b||!b.length)return a;for(var d={},e=0;e<b.length;e++)d[b[e]]=!!a[b[e]];return d}function k(a,b){if(!a&&0!==a)return a;for(var d={},e=0;e<b;e++)d[e+1]=!!(a&1),a>>=1;return d}function z(a){if(a&&a.length){for(var b={},d=0;d<a.length;d++)b[a[d]]=!0;return b}}if(c._has_global("__cmp")||c._has_global("__tcfapi")&&!c._has_global("_adroll_tcfapi_placeholder_installed"))c._install_cmp=function(){};else{c._cmp_calls=.[];c._set_global("__cmp",function(a,b,d){"ping"===a?d({gdprAppliesGlobally:!1,cmpLoaded:!1}):c._cmp_calls.push([a,b,d])});c._tcfapi_calls=[];c._set_global("__tcfapi",function(a,b,d,e){"ping"===a?d({gdprApplies:void 0,cmpLoaded:!1,cmpStatus:"loading",displayStatus:void 0,apiVersion:"2.0",cmpVersion:void 0,cmpId:void 0,gvlVersion:void 0,tcfPolicyVersion:void 0}):c._tcfapi_calls.push([a,e,d])});var m={getVendorConsents:function(a){var b=c._global("__adroll_consent"),d=c._global("__adroll_con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\internal[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	103674
Entropy (8bit):	5.172469992008471
Encrypted:	false
SSDEEP:	768:0j0Nps4FbAm2bA4mBKgxw/s+hClmMDS2c5DHS92W:Q0W4NIKHlmY
MD5:	A90D42358288605CDC44E3B087F2A86D
SHA1:	F950179C44BC363322A2C7AD45E67DAE2D7A9567
SHA-256:	A4B8761B4B77067BD7CE66BA56E4C451038A395C46406CDEECB94C062B1DA983
SHA-512:	4F5D1E5F19D8D5E7E41636B1EFE3D8E125017C7B194666AF4B990F91D3EC434C01C650F5BD85F334E6199306ABBF0A04DED71F1C2CAF28E6021B89BAB47FBED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/themes/custom/casella/css/custom/internal.css?qljrib
Preview:	/*..Website Name: Casella..Description: Internal Page specific stylesheet..Version: 1.0..Author: Adworkshop..Author URI: http://www.adworkshop.com..*/..../* ========== */../* HEADER */../* ========== */...internal-headerPanel-container {background: #0a253e; width: 100%; padding: 60px 0; text-align: left;}...internal-headerPanel-container h1 {color: #7abf23; font-size: 30px; text-transform: uppercase;}..../*Hero*/...internal-headerPanel-hero {color: #fff; font-size: 15px; line-height: 1.5; margin: 15px 0 0;}..../*BreadCrumbs*/...internal-headerPanel-breadcrumbs {display:none;}...internal-headerPanel-breadcrumbs:before {content:''; display:block; margin:25px 0 0; padding:30px 0 0; height:1px; width:225px; border-top:1px solid #45596c;}...internal-headerPanel-breadcrumbs ul li {display:inline-block; font-size:12px; font-family: 'Gotham-Bold'; color: #0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.hoverdir[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	9482
Entropy (8bit):	4.158127586191687
Encrypted:	false
SSDEEP:	192:bLL7RRl42nU7t7NncXOrdy32lMHPTipf/0Klxd1wIoTIQ2LM5tLbSk7WIC7:v5ykHLeb4mLURo
MD5:	A7C8D367551B1EF41C0B053A7941021D
SHA1:	D424A8006FFE78CB3928872594359D88A5F09EF4
SHA-256:	C9C4E7FAEF055A775BE35D8D48E1DBC0D9B9A1D5FC85CB40F7DCD04151B5F257
SHA-512:	0DC3D8FF54927CB9A7FDA1BB48B684ED48CACD65F80B9DFBD9C826298C3360228884AA0C22C86EB46FB740323487B6F39F5F50CD9B04C243ECB809C7FF3A722

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.hoverdir[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/plugins/hoverdir/jquery.hoverdir.js?v=1.1.2
Preview:	/**. * jquery.hoverdir.js v1.1.2. * http://www.codrops.com. *. * Licensed under the MIT license.. * http://www.opensource.org/licenses/mit-license.php. *. * Copyright 2012, Codrops. * http://www.codrops.com. */.(function (factory) {. 'use strict';. if (typeof define === 'function' && define.amd) {. define(['jquery'], factory);. } else if (typ eof exports !== 'undefined') {. module.exports = factory(require('jquery'));. } else {. factory(jQuery);. }.})(function ($) {. 'use strict';.. function Hoverdir(ele ment, options) {. this.$el = $(element);. // set options. this.options = $.extend(true, {}, this.defaults, options);. // initialize visibility to false for show and hide method. this.isVisible = false;. // get the hover for this element. this.$hoverElem = this.$el.find(this.options.hoverElem);. // transition properties. this.transitionProp = 'all ' + this.options.speed + 'ms ' + this.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86452
Entropy (8bit):	5.519029987848581
Encrypted:	false
SSDEEP:	1536:JM0YWtzcB0Q+HQafG5PuQU4/9E0GFadncI6c1K9ovKPiIZ1Au/2O:JM0vO0pu5PHGsdp6CtO
MD5:	63EAD9DBC25B10D046C76D54BE47EC73
SHA1:	9BC68DA5C0A2EBC9D803F5F243670CB21D42351E
SHA-256:	DAC68C294F00ADC1C9DCFE5D330054F806394AC67E744FE7EF418D96C113470A
SHA-512:	0D07C61079AD943096C8DB5065389CB144F9DE5EDEB82FF9F36408CF8713EC8EE8D5B6EF60341C8090CD9F4EB15556C2ADD7D415B1C02231B37A3303BCA774A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=AW-740347260
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],.. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],.. "predicates":[{. "function":"_eq",. "arg0":["mac ro",0],. "arg1":"gtm.js". }],.. "rules":[. [["if",0],["add",0]]],."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa ,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator& &a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},fa="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ha;.if(" function"==typeof Object.setPrototypeOf)ha=Object.setPrototypeOf;else{var ia;a:{var ka={a:!0},ma={};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\js[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	4.939382788025054
Encrypted:	false
SSDEEP:	48:xuteGV5lfKog8//NiQC+p4CHQC+pL0ZuteGV5lfKog8//NiQC+p4CHQC+pL0f:3GVPfKo1/ViQ7lQ7p4GVPfKo1/ViQ7lr
MD5:	A85C41C02753141C109ACEFE31C00D7E
SHA1:	FC232B89D8F2B30564DABCAF9501A492EBA9CD5B
SHA-256:	2BF81E7668A65B74F26F85ADA91423A569EA734D4FD42FC655411425BF1D5A78
SHA-512:	E5EA7F082FBF3FC51F460492CFC0FB0B355C51C85E28B469164D56650D93F79A8BACE01025D693D99AC2BAD3DA645CA836F067287490ED5ADB16E89E9D1393(
Malicious:	false
Reputation:	low
Preview:	(function() {.try {. (function(){./**/..})();.(function() {. try {. if (document.getElementById('mm_sync_back_ground')). return;. var frm = document.c reateElement('iframe');. frm.style.visibility = 'hidden';. frm.style.display = 'none';. frm.src = "https://pixel.mathtag.com/sync/iframe?mt_uuid=cc3a6091-a4b5-4a00-95ec-94d4d16e385b&no_iframe=1&mt_adid=187218&source=mathtag";. frm.setAttribute("id", "mm_sync_back_ground");. frm.title="MediaMath Advertisi ng";.. if (document.body). document.body.appendChild(frm);. else. if (document.head). document.head.appendChild(frm);. }. c atch(ex). {. document.createElement("img").src="//pixel.mathtag.com/error/img?error_domain=synciframe&what="+encodeURIComponent(ex.message);. }.})( );..}.catch(ex).{. document.createElement("img").src="//pixel.mathtag.com/error/img?error_domain=wrap_js&what="+encodeURIComponent(ex.mess

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\layout_css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	9793
Entropy (8bit):	5.291991402487626
Encrypted:	false
SSDEEP:	192:6CJnqhwg9gHK3LhOsIs6RGvjHc6ZUSUcUaUg8/XGYSV:IyRs6eckUSUcUaUg8/XGYSV
MD5:	2FD5941A631AB34A134BF89F4668EECF
SHA1:	2F0CA3A94CB613DC4A06A0F11418A6370EAB6808
SHA-256:	E6F964212202F35327DE4C81E86F731EC1F0774014F8461744F3E4277AB5FEFC
SHA-512:	7428580D81BF28407F5991EF467EA0F5A258101D5F4D73887631E049B56DDFC8DFC00D354377ADFA6815ECEEB199859EFC40A7275C76302E2B61442C9C458288
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\layout_css[1].css	
Reputation:	low
IE Cache URL:	http://https://secure3.i-doxs.net/casella/layout_css.css
Preview:	BODY..{.. PADDING-RIGHT: 0px;.. PADDING-LEFT: 0px;.. MARGIN-BOTTOM: 0px;.. PADDING-BOTTOM: 0px;.. MARGIN-LEFT: 0px;.. MARGIN-RIGHT: 0px;.. PADDING-TOP: 0px;.. FONT-FAMILY: Arial, Geneva, Helvetica, Verdana, Swiss, SunSans-Regular;.. BACKGROUND-COLOR: #E8EDF1..}..A..{.. FONT-WEIGHT: bold;.. COLOR: #002d62;.. TEXT-DECORATION: none;.. outline: none..}..A:visited..{.. TEXT-DECORATION: none; ..}..A:active..{.. TEXT-DECORATION: underline ..}..A:hover..{.. FONT-WEIGHT: bold;.. TEXT-DECORATION: underline..}..P..{.. FONT-SIZE: 12px;.. LINE-HEIGHT: 14px;.. MARGIN-RIGHT: 5px;.. COLOR: #5a636f..}..TD..{.. FONT-SIZE: 12px;.. LINE-HEIGHT: 14px..}..H1..{.. MARGIN-TOP: 0px;.. FONT-WEIGHT: bold;.. FONT-SIZE: 24px;.. MARGIN-BOTTOM: 0px;.. COLOR: white;.. LINE-HEIGHT: 44px..}..H2..{.. MARGIN-TOP: 5px;.. FONT-WEIGHT: bold;.. FONT-SIZE: 14px;.. MARGIN-LEFT: 22px;.. LINE-HEIGHT: 16px;.. MARGIN-RIGHT:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\match[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68
Entropy (8bit):	4.200601260429725
Encrypted:	false
SSDEEP:	3:yionv//thPlE+tnM09/Woz59tVp:6v/lhPfZM09tzjTp
MD5:	C4A2B870062C2BB98C500BC1526C0498
SHA1:	528666CCDB12997358077BC8FCDBFB6B825C7788
SHA-256:	2AA4FA20701CDD6D8D56046069001186B5267E3EE7D0EF618AD2F4A683723E11
SHA-512:	2F1A3ABCD12125F7EF18D61A960901C0FD6F82DD02EA2B8041859E6D5F0A7F08DB17CC110DC6D8A3F7D0D1BA790C4BCCA2506D3C60EDFEB5CB29433E9F4F72E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....IDATx.c`.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\modernizr.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7059
Entropy (8bit):	5.307190209270235
Encrypted:	false
SSDEEP:	96:44uuITey2hGUupREEp3DD1sd/+B6C6mnt4mQIFM4mHsi97kKP4IZSp0xQHn:YuIT/2hHEpzDG9nenONIFwHseA70xQHn
MD5:	D0FB33DCF799E36A31CE24795CD9FD16
SHA1:	5E4FB5F00EDF27996C33307A773523C693E614BA
SHA-256:	895385A514223CB5636F335DC52A67F80E6A3D7E61D7ED0BD3D2D4E16A12225A
SHA-512:	6995DBC7D50BEFD1ECAAAD9F653090648B171CF8F4C663DBF5ADDE8D19E89A1DEA7A353EEC4943C02C692C9BA8C55223D50FE72CFDB6ED296142EF0822B7FA6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/js/libs/modernizr.min.js?v=3.3.1
Preview:	/*! modernizr 3.3.1 (Custom Build) | MIT *. * https://modernizr.com/download/?-csstransitions-details-inputtypes-svg-touchevents-addtest-mq-prefixes-setclasses-teststyles !*/.!function(e,t,n){function i(e,t){return typeof e===t}function o(){var e,t,n,o,r,s,a;for(var l in _)if(_.hasOwnProperty(l)){if(e=[],t=_[l],t.name&&(e.push(t.name.toLowerCase()),t.options&&t.options.aliases&&t.options.aliases.length))for(n=0;n<t.options.aliases.length;n++)e.push(t.options.aliases[n].toLowerCase());for(o=i(t.fn,"function")?t.fn():t.fn,r=0;r<e.length;r++)s=e[r],a=s.split("."),1===a.length?Modernizr[a[0]]=o:(!Modernizr[a[0]]||Modernizr[a[0]]instanceof Boolean||(Modernizr[a[0]]=new Boolean(Modernizr[a[0]])),Modernizr[a[0]][a[1]]=o),C.push((o?"":"no-")+a.join("-"))}}function r(e){var t=b.className,n=Modernizr._config.classPrefix||"";if(S&&(t=t.baseVal),Modernizr._config.enableJSClass){var i=new RegExp("(^|\\s)"+n+"no-js(\\s|$)");t=t.replace(i,"$1"+n+"js$2")}Modernizr._config.enableClasses&&(t+=" "+n+e.jo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\modernizr.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	7063
Entropy (8bit):	5.311179289186801
Encrypted:	false
SSDEEP:	96:B49uITey2hGUupREEp3DD1sd/+B6C6mnt4mQIFM4mHsi97kKP4IZSp0xQHy:quIT/2hHEpzDG9nenONIFwHseA70xQHy
MD5:	F645839E3438709E823AAB1C099CA223
SHA1:	DF4653A3CB0E47AE5969ED8CE28F73147DCDD8D6
SHA-256:	F1F852A254973D33784F79AEB42BF571478033DF82DD9B96F3E28E148541D7D7
SHA-512:	1A1E7ED446E507AC2FED3580E138A727A9BF1AA2B1D961E6207EC6C594254D8BAE7DF5CEAEC201B026B0FEE9AB6127D4E6F0D2C5FB616D11EAD829E564EFA751
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/themes/custom/casella/js/libs/modernizr.min.js?v=3.3.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\modernizr.min[2].js	
Preview:	/*! modernizr 3.3.1 (Custom Build) | MIT *.. * https://modernizr.com/download/?-csstransitions-details-inputtypes-svg-touchevents-addtest-mq-prefixes-setclasses-teststyles !*/..!function(e,t,n){function i(e,t){return typeof e===t}function o(){var e,t,n,o,r,s,a;for(var l in _)if(_.hasOwnProperty(l)){if(e=[],t=_[l],t.name&&(e.push(t.name.toLowerCase( )),t.options&&t.options.aliases&&t.options.aliases.length))for(n=0;n<t.options.aliases.length;n++)e.push(t.options.aliases[n].toLowerCase());for(o=i(t.fn,"function")?t.fn ():t.fn,r=0;r<e.length;r++)s=e[r],a=s.split("."),1===a.length?Modernizr[a[0]]=o:(!Modernizr[a[0]]||Modernizr[a[0]]instanceof Boolean||(Modernizr[a[0]]=new Boolean(Moderni zr[a[0]])),Modernizr[a[0]][a[1]]=o),C.push((o?"":"no-")+a.join("-"))}}function r(e){var t=b.className,n=Modernizr._config.classPrefix||"";if(S&&(t=t.baseVal),Modernizr._c onfig.enableJSClass){var i=new RegExp("(^|\\s)"+n+"no-js(\\s|$)");t=t.replace(i,"$1"+n+"js$2")}Modernizr._config.enableClasses&&(t+=" "+n+e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ndqfonticons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), ndqfonticons family
Category:	downloaded
Size (bytes):	64264
Entropy (8bit):	6.201521235202019
Encrypted:	false
SSDEEP:	1536:AwoSpG7xWGNIJWfYQa2ksTZ9fLgW4Ahoi7WXQaOhbC6CHCG2c9qoGzjPtEjFPQmW:AwTpG7XIJWfYQ9PzfLgW4Ahoi7WXQaOD
MD5:	B3A284884E0C8DE8919A361416172AEB
SHA1:	A8F26846276F67CEDF8FBA94DA54E2E8B6C4D5FE
SHA-256:	4AA87B2D813B5D836F7A59AF064A7326C6D7B8A06DD5B37617EFB6AFFB2C13E1
SHA-512:	6C28ABBB84BC080DD0D43BE898C9F8CCB521DE100FAEAC5D1A14FF225683B54B32E438903C755EACB59FE72606F0E63D765795A0F115CD9B18413C5B9AA6CE 47
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ir.casella.com/profiles/nasdaqir/themes/custom/nir_base/dist/fonts/ndqfonticons.eot
Preview:	....P.....LP.....n.d.q.f.o.n.t.i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....n.d.q.f.o.n.t.i.c.o.n.s.....PFFTMq.....4....GDEF.S... ..... OS/2/.M\...X...Vcmap.....rgasp.....glyfn.....@head..`.....6hhea.0.....$hmtx:/7.....Tloca.....x...Nmaxp.....8... name.v.....posta9.....=....._.<.... .....&.....@.....L.f...G.L.f.....PfEd.@.....;.;.R.....v.\.\.D.f.....|.D.3.3. 3.J.g.\.9...g.).F.U.P...\.\.\.\.\.D.D.D.....\.D.D.D.D.D.....w.w.....U.f.f...u.P./.....z...w.D.K.K.K.K.K.K...F.F.P...P."...D.+.U.D.U.U.o.V.S.U.U.U.U.U.U.U.U.U.3.3.U.,.C. f.E.f.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.k.K.H.H.H.H.K.U.K.K.K.K.J.K.Q.K.K.H.K.H.H.H.H.H.H.K.H.I.f.t.t.<.<.D.D.D.D.D.D.D.H...6.D.D.H.D.H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nr-1208.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	31332
Entropy (8bit):	5.307480606148579
Encrypted:	false
SSDEEP:	384:bW+ioYSXVnMGIhDlu7kKuaq9VB5gwlfy9StcepgYYKxsq6lM7Y0vncYemRhVxp8q:bW5Laq9VHTZDhumdcfKtCK/
MD5:	1A71E4208296F97B465116492F59124D
SHA1:	40C8559838A758630287ED0B0F8E4E076215BDB0
SHA-256:	4014CA31D3C8E768608A40ED160A405AE39836A5B2C43F256BEE3BDF427DD67F
SHA-512:	2E5853FBD0D19FE6C69D8B3106F1788A1AB2483202FAC40D8303E74925D4632E91E66B40D3FB37802E59269EE715D5EF8BFB92BAE65E215D0D67BB29D55B4C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js-agent.newrelic.com/nr-1208.min.js
Preview:	!function(n,t,e){function r(e,i){if(!t[e]){if(!n[e]){var a="function"==typeof __nr_require&&__nr_require;if(!i&&a)return a(e,!0);if(o)return o(e,!0);throw new Error("Cannot find mo dule '"+e+"'")}var s=t[e]={exports:{}};n[e][0].call(s.exports,function(t){var o=n[e][1][t];return r(o||t)},s,s.exports)}return t[e].exports}for(var o="function"==typeof __nr_requir e&&__nr_require,i=0;i<e.length;i++)r(e[i]);return r}({1:[function(n,t,e){t.exports=function(n,t){return"addEventListener"in window?window.addEventListener(n,t,!1):"attach Event"in window?window.attachEvent("on"+n,t):void 0}},{}],2:[function(n,t,e){function r(n,t,e,r,i){var a=c(n,t,e,i);return a.metrics=o(r,a.metrics),a}function o(n,t){return t||(t={ count:0}),t.count+=1,m(n,function(n,e){t[n]=i(e,t[n])}),t}function i(n,t){return t?(t.c||(t=u(t.t)),t.c+=1,t.t+=n,t.sos+=n*n,n>t.max&&(t.max=n),n<t.min&&(t.min=n),t):{t:n}}function a(n,t,e,r,o){var a=c(n,t,r,o);if(!a.metrics)return void(a.metrics=e);var u=a.metrics;u.count+=e.count,m(e,fun

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\organics[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	18542
Entropy (8bit):	5.055963360050615
Encrypted:	false
SSDEEP:	192:48lkgEDj1YbWeKeGtFfc5uDne7DFqgCwFdyFGFeFecttiS19z9/XdvM6mSltVmG3:zHgEDjm+F8HFdyFGFeFecBlxtv+iLcU
MD5:	620CF72707B8D7358EC1DE4A1F3900B6
SHA1:	9684EA611F4E14D511D03034D4426D4DA3B027A0
SHA-256:	AAA821699241EDB24FFD4C2814BA9A1822B86C33E96A7FD418C1B776E390E299
SHA-512:	0C546543458AB64D991B174D7FE8AF50FBD0E37FA402D1EA5E202ABFE3CEE4F69442D9D6488D1AC8DD65C1BEB4BBF49E67B4069A3A178582E4757EA195E74F CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/css/custom/organics.css?qpcosx

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\organics[1].css	
Preview:	/*.Website Name: Casella.Description: Organics specific stylesheet.Version: 1.0.Author: Adworkshop.Author URI: http://www.adworkshop.com.*/.. .sectionWrapper { width:100%;}../* ========== */./* SECTION NAVIGATION */./* ========== ========== */ . #sectionNav {position:relative; padding:0; background: #00263d; z-index:2000; border-bottom: 1px solid #76be43;}. . #sectionNav .sectionNav-logoContainer {position: relative; z-index: 2;display:inline-block; padding:20px 0; line-height:0;}. #sectionNav .sectionNav-logoContainer a {. display:inline-block; width:375px; height:auto;. -webkit-transition: all .3s ease-in-out; -moz-transition: all .3s ease-in-out; -o-transition: all .3s ease-in-out; -ms-transition: all .3s ease-in-out; transition: all .3s ease-in-out;. }. #sectionNav .sectionNav-logoContainer a:hover {opacity:.7;}. #sectionNav .sectionNav-logoContainer img {wid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\paragraphs.unpublished[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	57
Entropy (8bit):	4.5736893560802265
Encrypted:	false
SSDEEP:	3:kEUWKSnkmFmGOCXLFSKPkRtv:kEUxIF/hRk7v
MD5:	6BF7857DC423EADA40DDF4AEC0506587
SHA1:	9DE57D9EF96077986EFFBAB3521672BD15736488
SHA-256:	F1EEA94C1D7F9C6747515E1D7AF60618498E8197905F290BC3851DA41FBD5588
SHA-512:	74DBA740C9898FEB942047E576E29FB9CF5C7AAFBC2E6F8D0488AC1062864947BF93A141973B167C0554AD887BD10A463597782AE73860242A255FC958891CC1
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/modules/contrib/paragraphs/css/paragraphs.unpublished.css?qpcosx
Preview:	.paragraph--unpublished {. background-color: #fff4f4;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\payBill-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 281 x 154, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2696
Entropy (8bit):	7.806391272870825
Encrypted:	false
SSDEEP:	48:i3b8EeOpzNyxkadra2YP5IdF4IBFzSViz9ZjeA0wVuVil7jWpWSbDjmpX/j:k98HM2hv4IXLZyAmViRjWpnmJ/j
MD5:	24173167A16F35E3591641C590ABC3EF
SHA1:	7FF1BC54EED49E3F9BB336974C1225BD2A6532B7
SHA-256:	2F21D45231796FC8762D0F59237F3B5A4059F2F94CD8A48E172B84267B732AAD
SHA-512:	2280D928A57C711EEB5B2762DCA36D0E8E764CECF6EFBB00B3F754BAF1C8ECAFD20357C9BEC89E349A5101E80B1D61FFFA0A0BEEBD0184FD5EEA615B74FDE279
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/themes/custom/casella/i/misc/payBill-icon.png
Preview:	.PNG.....IHDR.....C<.....tEXtSoftware.Adobe ImageReadyq.e<...*IDATx...u....9....c*XR.@..T0P.&.@*HR.l.a*.T.RA...[..;.y....6..-}.9:..@.e..,Ky.....C.1p....)..|..$l]..... .".\.N.E.2v.e.y.;..|:.l..@.b.X..H...J.....\&.....J.....,/....)...&.pB$\..#l.+n.<.....e.{*.E....O..S.w...~G.`]a\e..@.r....w.Z!R.se7.d....E.M..(_,...aJ.r.i..c.i....:rBD.....qe,..Z...&...Q...d ...BI.....P0.m..t.\iT.k...dbj.BG..C.,.m.KW.Z#..D2.f.p.C@d...@.=..8..Hf.t?M~pR.3.` ,R.6.....o.L.|=.t.`..(...#er.}S.F2.!..r..`...KE2:8..@H.....`i..){...f....n:.C...9{..r{:{.`...K...g/..@y .HD3.5.&.7:+F3&...j.f..$.!zW..."....@.....]...}?k.K.29...m.%.....n.k..\|n.4?..U...<n..fn.V.SE.jp....G1..O.5.H...u..'..C2.fRC3.-,..6<K....l.c.~.Z.B2..\-.....t.@..L..t)..Hb.hs..M... ...@62.E...{....H.....^.{.P.&.g'TT3....d.+Q.0.3:}..K+&|..FV..&$.)3....P..*.F".Q..D3H.....D1.....i>...w.#. .yY.i..B.$...'MH.....o9....\u.<T4.....J4.uY6.~..Y#...x..x~..$..xs.7..j.!5.. J..Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\position-container.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	95
Entropy (8bit):	4.220495863964869
Encrypted:	false
SSDEEP:	3:USQTWqVYb1MVNMNQMXm/1JrYv:UVtYbymQt/frYv
MD5:	A203BFB5819742D466B5E99AF480009A
SHA1:	CC0323B65FD726EF89264B2A7A6D3D7C4999A5E2
SHA-256:	92931CEB6A0AD1C9B3E8FC6F335B9DFD6F0C7C8EE36F089BB10241C142A78FAA
SHA-512:	D12FB20EDE3211C3C3469D5DC86E2BE654A3D5ACE2FE3F20D3E959596106E0775369CB1A5A1886447497508DD572F4D61A47291EDD25910DD8713883AD01518
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/core/themes/stable/css/system/components/position-container.module.css?qpcosx
Preview:	/*. * @file. * Contain positioned elements.. */...position-container {. position: relative;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\redir[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUkwx7tHh/:fD/
MD5:	221D8352905F2C38B3CB2BD191D630B0
SHA1:	D804B495CB9B84B9007A25B5D85F9AE674004CDE
SHA-256:	89FE0EE6020314794FC2CFEACF3D10C31050CFE56F8EBDDF1ED0A33FBE941FA7
SHA-512:	CB3397776F5CA1D15D24786896B2478C6548D0B14DEC0832BFB16C4C419135300704F8A7A4DFBF56D625429C1598EE8110958648F25A3CCA09E6956C1FD3335F
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\reset-appearance.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	274
Entropy (8bit):	4.5219236059353545
Encrypted:	false
SSDEEP:	6:UiE4nzwfgWczGPtd+LRuL7OAnRtX0H0D0K:UvdczGPtELRuL7jXOMH
MD5:	5318929554D3BCE84406B2A5418EACAE
SHA1:	0E6DB18A3D7FBBDB6FC3827D3DA529A778AED732
SHA-256:	0AC01AB832B811CDC2DFDDAF28BA2F1EE3EF3BB6486CBAEB424226FDE71EE625
SHA-512:	9CD234CAFB5B728B9F0C7D1E2A9E851A751C1617B04550E68ECB0DD0E7211FBC6453093E5AC93CBACA89F716AA573BEACFE730917F567619DC93675A52F08C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/core/themes/stable/css/system/components/reset-appearance.module.css?qpcosx
Preview:	/*. * @file. * Utility class to remove browser styles, especially for button.. */...reset-appearance {. margin: 0;. padding: 0;. border: 0 none;. background: transparent;. line-height: inherit;. -webkit-appearance: none;. -moz-appearance: none;. appearance: none;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\roundtrip[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	42078
Entropy (8bit):	5.404500116886135
Encrypted:	false
SSDEEP:	768:2i5UOTGnoBVKQlhGIDITmxJCC4/xbGYtcZ9fuie6pc+tS2C:hU4HKQKfkMZbSV
MD5:	4748055DBDD5649BB8F3F2A9B89F85B1
SHA1:	5D5B298C45DF22FEAA07B87B11BBC88E71529265
SHA-256:	F55B80216D81F421D8DA8C69AE09068B1231E4B0FB6D3912EAE8D147B5232D9C
SHA-512:	8784022191246AAC6A7A5EAB2211C3D5C23B9FB479D4B0637C7D5A9A04B80598E8E067FCC9EF9AF3F51BE5437E143472D69CB02AC4BDDEAE35427EA15F1D642
Malicious:	false
Reputation:	low
IE Cache URL:	http://a.adroll.com/j/roundtrip.js
Preview:	window.__adroll||(function(){function f(){this.version="1.0";this.exp=8760;this.eexp=720;this.pv=1E11*Math.random();this.__adc="__ar_v4";this._nad=0;this._lce=null;this._loaded=this._broken=!1;this._url=2E3;this._kwl=300;this._r={};this.cm_urls=[];this._logs=[];this.consent_networks={facebook:"f",linkedin:"linkedin"};for(var a=Array(4),b=0;b<a.length;b++)a[b]=(Math.round(1E11*Math.random()).toString(16)+Array(9).join("0")).substr(0,8);this._set_global("adroll_sid",a.join(""));this._has_global("adroll_adv_id")&&(this.load_experiment_js(),.this.init_pixchk(),this._load_precheck_js(),this.trigger_gtm_consent_event(),this.load_pixel_assistant(),["adroll_adv_id","adroll_pix_id"].forEach(function(a){window.hasOwnProperty(a)&&("string"===typeof window[a]||window[a]instanceof String)&&(window[a]=window[a].replace(/[^A-Z0-9_]/g,""))})};f.prototype.load_consent_banner=function(){window.document.getElementById("__adroll_consent_banner_el")||this.add_script_element("s.adroll.com/j/consent_tcfv2.j

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\roundtrip[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	42078
Entropy (8bit):	5.404500116886135
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\roundtrip[2].js	
SSDEEP:	768:2i5UOTGnoBVKQIhGIDITmxJCC4/xbGYtcZ9fuie6pc+tS2C:hU4HKQKfkMZbSV
MD5:	4748055DBDD5649BB8F3F2A9B89F85B1
SHA1:	5D5B298C45DF22FEAA07B87B11BBC88E71529265
SHA-256:	F55B80216D81F421D8DA8C69AE09068B1231E4B0FB6D3912EAE8D147B5232D9C
SHA-512:	8784022191246AAC6A7A5EAB2211C3D5C23B9FB479D4B0637C7D5A9A04B80598E8E067FCC9EF9AF3F51BE5437E143472D69CB02AC4BDDEAE35427EA15F1D64 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.adroll.com/j/roundtrip.js
Preview:	window.__adroll||(function(){function f(){this.version="1.0";this.exp=8760;this.eexp=720;this.pv=1E11*Math.random();this.__adc="__ar_v4";this._nad=0;this._lce=null;this._ loaded=this._broken=!1;this._url=2E3;this._kwl=300;this._r={};this.cm_urls=[];this._logs=[];this.consent_networks={facebook:"f",linkedin:"linkedin"};for(var a=Array(4),b= 0;b<a.length;b++)a[b]=(Math.round(1E11*Math.random()).toString(16)+Array(9).join("0")).substr(0,8);this._set_global("adroll_sid",a.join(""));this._has_global("adroll_adv_ id")&&(this.load_experiment_js(),.this.init_pixchk(),this._load_precheck_js(),this.trigger_gtm_consent_event(),this.load_pixel_assistant(),["adroll_adv_id","adroll_pix_id "].forEach(function(a){window.hasOwnProperty(a)&&("string"===typeof window[a]||window[a]instanceof String)&&(window[a]=window[a].replace(/[^A-Z0-9_]/g,""))})); f.prototype.load_consent_banner=function(){window.document.getElementById("__adroll_consent_banner_el")||this.add_script_element("s.adroll.com/j/consent_tcfv2.j

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rum[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21E FDC
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sd[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.9889835948335506
Encrypted:	false
SSDEEP:	3:CUkxl7/lHh/:slf/
MD5:	B4491705564909DA7F9EAF749DBBFBB1
SHA1:	279315D507855C6A4351E1E2C2F39DD9CD2FCCD8
SHA-256:	4E0705327480AD2323CB03D9C450FFCAE4A98BF3A5382FA0C7882145ED620E49
SHA-512:	B8D82D64EC656C63570B82215564929ADAD167E61643FD72283B94F3E448EF8AB0AD42202F3537A0DA89960BBDC69498608FC6EC89502C6C338B6226C8BF5E14
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sticky-header.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	163
Entropy (8bit):	4.711564923747027
Encrypted:	false
SSDEEP:	3:UV91G2AVgULbvlFPFlHgQEBYPiK0EcIAFwF0Sf4IAwHEZCXLFSKPxC:UNGgiqBYqKhgwF0SwIjlhRw
MD5:	47DD1A9AB77932B92B6C8E68B9B41E77
SHA1:	EE55F889A03FDCF021FA916B6B7CFED8DB417249
SHA-256:	0B61E01FA0FA02EBA3C6A074427DDF2A6CF98C01727B2796309B2B5B005FAC70
SHA-512:	29F9277A71D16CAF1EC6EA5E70963D8F98EFCFCC92F34EDDDD1F669753255386508811 3A66B22BE830DE6EF534128527AB18400C9ACF34BA031EA6FEF82FB57
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/core/themes/stable/css/system/components/sticky-header.module.css?qpcosx

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sticky-header.module[1].css	
Preview:	/**.. * @file.. * Table header behavior.. *.. * @see tableheader.js. */..table.sticky-header {.. z-index: 500;.. top: 0;.. margin-top: 0;.. background-color: #fff;..}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\system-status-report-counters[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	584
Entropy (8bit):	4.839526368513175
Encrypted:	false
SSDEEP:	12:U6dfNKgteFEYKWJoIXmed6GrqvmRNa29GKgFK:3dRtY2Vl2eQTvYNanW
MD5:	E65CC16D5C92CD242850D0D607CE3B61
SHA1:	CFE0AB80E76AB1FDE9B226C51E425587DE708C9B
SHA-256:	791BF430E835E8F755420AAC9D175BB568B165DBBA709453EB2E48C4A479AA63
SHA-512:	6FB24AAB9FAF4E9419A5464D02E47A726AECB32321417F080F5AF806F3DE5B07C0FCC870051E4FF284282B0C1EBB2BEFE92F20648B9B5406EFAEFD5C6930E956
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/core/themes/stable/css/system/components/system-status-report-counters.css?qljrib
Preview:	/**.. * @file.. * Styles for the system status report counters... */.....system-status-report-counters__item {.. width: 100%;.. margin-bottom: 0.5em;.. padding: 0.5em 0;.. text-align: center;.. white-space: nowrap;.. background-color: rgba(0, 0, 0, 0.063);..}....@media screen and (min-width: 60em) {.. .system-status-report-counters {.. display: flex;.. flex-wrap: wrap;.. justify-content: space-between;.. }.. .system-status-report-counters__item--half-width {.. width: 49%;.. }.. .system-status-report-counters__item--third-width {.. width: 33%;.. }..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\system-status-report-general-info[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	269
Entropy (8bit):	4.758561643554257
Encrypted:	false
SSDEEP:	6:U6dqbADEnCWRK2y7fy7Mm5AUu/NIRYYfmy7MmIAFfNg/RYYy:U6dfYntRj+fyIm5AB/NIXfmyImIA5lXy
MD5:	5F4C9A3373FD14DF9E7FDCD2C3D91204
SHA1:	D04D743B35759D8DDBDFB9639C9D991033CF1356
SHA-256:	8EF76C600A3610E1D312FFD41BEAF00A4D92A4ED232624B7840E0833F912A137
SHA-512:	F8FDFF9AFF7B0EF8103FD7D17DB3A344DD4001DB4402D30B7536F7B99434345A0ADD34BFAC1269FCE5E59C1F5086FF2600F639304E47FFC3FE5A593C0F35931
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c-11158-20201221-www-casella-com.i.icims.com/core/themes/stable/css/system/components/system-status-report-general-info.css?qljrib
Preview:	/**.. * @file.. * Default styles for the System Status general info... */.....system-status-general-info__item {.. margin-top: 1em;.. padding: 0 1em 1em;.. border: 1px solid #ccc;..}.....system-status-general-info__item-title {.. border-bottom: 1px solid #ccc;..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\tDbV2oqRg1oM3QBjjcaDkOJGiRD7Owc[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 29856, version 1.1
Category:	downloaded
Size (bytes):	29856
Entropy (8bit):	7.9847589176034734
Encrypted:	false
SSDEEP:	768:a09Vn3v9YqS3LDmiUuLhiHdcng0vn/i+l:a2vBS7DCuLoHdC/Bl
MD5:	176F838635C53CBE9BE7B8A649CE7B1A
SHA1:	E7E133B0CB9155C84B43447E76404F83EAD76A57
SHA-256:	81656FAE16BC170A071115EF76F8D15469D3B9013497B10B7656035E40584DC3
SHA-512:	165C4F0090BE6CA1B392EBEBF25305730CEDAEC8EBEDD22FCC07DA62E85CBDDA92B6E3B70E24038E9122BCEF6692A28C8E43FCD41459138FB21AE55794BE955B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/droidserif/v13/tDbV2oqRg1oM3QBjjcaDkOJGiRD7Owc.woff
Preview:	wOFF.....t.....GDEF.....GPOS.....T...GSUB...x.....l.t.OS/2.....V...`....cmap.....j....mag.cvt ...X.....L..fpgm.....&....s.#.gasp.....glyf.. ....a....h....head..l....5...6..g.hhea..l.....$....hmtx..m.....L..=!loca..o.....C7i!maxp..p.... ... ...$name..p.....%xB)post..q....Y.....;prep..s.....x.e.....x.L ....q.@.x.....g.m.....e.v....vrs..7..R.F....ZB.. ..`.....''&t. ...C..A..8...Hk$..3Q.._.5....K\|=..t(z...K..k.....5....).P.....t..8gk../g...N..... .....Em''....&4%...(E/zS..V..V.!V..''....@U&Yu.. .lc'..g.9...p.s..&...C..3^..\|`.l....l.....zm.Fm.fm.R.P.(Ul....F.d_h..j.....3.<.I}..U?.....8.....c.p~P.tXGtL.uB'uJ.}.....;..{...z..z..z...>..g...\].W.....q...w).Mp.}.p...i.....i.t2.yq=..... ..F.:..,c..(.R.e...w.x...WSC-u..@..M.>.....Ca...T....l.Zz...QO../&.V.m$H.''M.,9..(r..\.:7..m.....G.e4../.3r.x.nD../....1...C.aWM5+.Xa.J(..i.....VSC-u..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\tabledrag.module[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\tabledrag.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1840
Entropy (8bit):	4.979542674814808
Encrypted:	false
SSDEEP:	48:02cxDZDI4f1Ba4fgwrE3QA1R53934s44XG4046XfX0u:02cxe4Xa4brE3r1L3t4j4W4046vku
MD5:	E5C74E1C6FD604D03DC784CF615E849B
SHA1:	A2F9F7270EA674F70A6702F5CE4201106EF398D9
SHA-256:	8188BAD0F77AAF0E06C5D199B36C85263048A4AC6361BED201939FDAB3DD196F
SHA-512:	4B47BF98B65F151AA42628A3E3BC69770AF9BD684900971F329059B396AFA83F549FD345D94BA2F1C6DE3726A8B9B21BCCB4399AD1A330903613A9417AB864CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.casella.com/core/themes/stable/css/system/components/tabledrag.module.css?qpcosx
Preview:	/**. * @file. * Table drag behavior.. *. * @see tabledrag.js. */..body.drag {. cursor: move;.}.tr.region-title {. font-weight: bold;.}.tr.region-message {. color: #999;.}.tr.region-populated {. display: none;.}.tr.add-new .tabledrag-changed {. display: none;.}..draggable a.tabledrag-handle {. float: left; /* LTR */. overflow: hidden;. height: 1.7em;. margin-left: -1em; /* LTR */. cursor: move;. text-decoration: none;.}.[dir="rtl"] .draggable a.tabledrag-handle {. float: right;. margin-right: -1em;. margin-left: 0;.}.a.ta bledrag-handle:hover {. text-decoration: none;.}.a.tabledrag-handle .handle {. width: 14px;. height: 14px;. margin: -0.4em 0.5em 0;. padding: 0.42em 0.5em;. backgro und: url(../../../images/core/icons/787878/move.svg) no-repeat 6px 7px;.}.a.tabledrag-handle:hover .handle,.a.tabledrag-handle:focus .handle {. background-image: url(../ ../../images/core/icons/000000/move.svg);.}..touchevents .draggable td {. padding: 0 10px;.}..touchevents .draggable .m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\tpid=cc3a6091-a4b5-4a00-95ec-94d4d16e385b[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	49
Entropy (8bit):	3.176789192964165
Encrypted:	false
SSDEEP:	3:CUVAae/XExlHrfx/n:8aOUJ/n
MD5:	56398E76BE6355AD5999B262208A17C9
SHA1:	A1FDEE122B95748D81CEE426D717C05B5174FE96
SHA-256:	2F561B02A49376E3679ACD5975E3790ABDFF09ECBADFA1E1858C7BA26E3FFCEF
SHA-512:	FD8B021F0236E487BFEE13BF8F0AE98760ABC492F7CA3023E292631979E135CB4CCB0C89B6234971B060AD72C0CA4474CBB5092C6C7A3255D81A54A36277B48
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....T..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\us[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	49
Entropy (8bit):	3.0021975300504877
Encrypted:	false
SSDEEP:	3:CUO/RD/wlHrfx/n:oD2/n
MD5:	ED280A0EA3CC38F3CBBC747ACFBEF47D
SHA1:	6BDCB32EE75E957A5085C010F4DFD0C716BFDADC
SHA-256:	8F69E10876805B747A3AD08A818D46AC7E731B1AF417EA6E259D9B6B7DEB65C5
SHA-512:	4248E293BB759C3AC0EA71F545E10E85D0C3C7F1237CE8B18C6A3FD00499A11BDC0252C938BE87359FA673C8E7A83C7CC6FC5D12718A68844C2615E5DCA352B
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....T..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\174173569_10159695018988888_4668211343051673706_n[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 720x540, frames 3
Category:	downloaded
Size (bytes):	83403
Entropy (8bit):	7.988791939956067
Encrypted:	false
SSDEEP:	1536:BfjIIGUAPlMjHtcX7vlP0bO+QyJsIZGW6AQXMZs7n3Cc7rqQcNxixHdL41tynm:3Kl2KBP0lhZBqXl+3/Vc7k9L41Unm
MD5:	A65908D93EBFCB23DB96CCBFD3B935E8
SHA1:	D15C2C7EB4A6AE23176392719B15243F0622E226

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\174173569_10159695018988888_4668211343051673706_n[1].jpg	
SHA-256:	FAAD471F95F653E0D3685D76B8E499841128C9D8E38B508A70DED430B94676ED
SHA-512:	23DAE4304C6F74FAC8F15B289ECB71F3D00081B08B316D471255DC72BD994CDEBD08EFF43A28980E4D4DCA29D8C1C15201EDFC753334740B3B4D2EBEB1039 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scontent-bos3-1.xx.fbcdn.net/v/t1.6435-0/p180x540/174173569_10159695018988888_4668211343051673706_n.jpg?_nc_cat=102&ccb=1-3&_nc_sid=110474&_nc_ohc=lm1f-dYLkN8AX-Lpn8i&_nc_ht=scontent-bos3-1.xx&tp=6&oh=0ca72c7f50f0b8016177ebf2159d6c98&oe=609E61C3
Preview:	.....JFIF.....Photoshop 3.0.8BIM.....g..jPkhjI42-vwMnSIE5-eZ..(.bFBMD0a000a88010000ff180000373f0000e6460000924f0000db7c000017bd0000cfc1 00001ccb0000cad40000cb450100...C.....%...#... , #&')*)..-0-(0%()(...C.....(...(((((((

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:47:00.434928894 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.434942961 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.434957981 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.434987068 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.435015917 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.435049057 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.435095072 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.514453888 CEST	49734	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.522676945 CEST	49736	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.522991896 CEST	49737	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.525769949 CEST	49738	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.525876045 CEST	49739	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.569571018 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.569628954 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.569654942 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.569669962 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.569705009 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.569716930 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.569741011 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.569760084 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.569806099 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.569864035 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.638067007 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.651475906 CEST	80	49734	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.651591063 CEST	80	49734	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.654371023 CEST	49734	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.656060934 CEST	80	49736	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.656196117 CEST	49736	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.658571005 CEST	80	49738	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.658694029 CEST	49738	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.660012007 CEST	80	49737	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.660104990 CEST	49737	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.660206079 CEST	49736	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.660324097 CEST	49734	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.660341024 CEST	49738	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.661319017 CEST	49737	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.662046909 CEST	80	49739	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.662153006 CEST	49739	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.664025068 CEST	49739	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.676242113 CEST	49745	80	192.168.2.4	65.9.66.129
May 4, 2021 21:47:00.678157091 CEST	49746	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.679081917 CEST	49747	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.683490038 CEST	49744	80	192.168.2.4	65.9.66.129
May 4, 2021 21:47:00.716830969 CEST	80	49745	65.9.66.129	192.168.2.4
May 4, 2021 21:47:00.716995955 CEST	49745	80	192.168.2.4	65.9.66.129
May 4, 2021 21:47:00.717621088 CEST	49745	80	192.168.2.4	65.9.66.129
May 4, 2021 21:47:00.724133015 CEST	80	49744	65.9.66.129	192.168.2.4
May 4, 2021 21:47:00.724399090 CEST	49744	80	192.168.2.4	65.9.66.129
May 4, 2021 21:47:00.725308895 CEST	443	49746	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.725418091 CEST	49746	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.726015091 CEST	443	49747	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.727055073 CEST	49747	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.727313995 CEST	49746	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.735649109 CEST	49747	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.758141994 CEST	80	49745	65.9.66.129	192.168.2.4
May 4, 2021 21:47:00.771056890 CEST	80	49735	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.771184921 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.772834063 CEST	49735	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.774245024 CEST	443	49746	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.776845932 CEST	443	49746	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.776895046 CEST	443	49746	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.776953936 CEST	443	49746	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.776993990 CEST	49746	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.777029991 CEST	49746	443	192.168.2.4	169.50.137.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:47:00.782712936 CEST	443	49747	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.785198927 CEST	443	49747	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.785275936 CEST	443	49747	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.785334110 CEST	443	49747	169.50.137.179	192.168.2.4
May 4, 2021 21:47:00.785336971 CEST	49747	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.785365105 CEST	49747	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.785378933 CEST	49747	443	192.168.2.4	169.50.137.179
May 4, 2021 21:47:00.793092012 CEST	80	49738	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.793148994 CEST	80	49736	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.793289900 CEST	80	49736	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.793368101 CEST	49736	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.793433905 CEST	80	49738	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.793538094 CEST	49738	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.797482967 CEST	80	49734	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.798285007 CEST	80	49737	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.798541069 CEST	49734	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.798573017 CEST	80	49737	52.87.65.167	192.168.2.4
May 4, 2021 21:47:00.798656940 CEST	49737	80	192.168.2.4	52.87.65.167
May 4, 2021 21:47:00.800043106 CEST	80	49739	52.87.65.167	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:46:59.949779034 CEST	192.168.2.4	8.8.8.8	0xe6a9	Standard query (0)	www.casella.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.580293894 CEST	192.168.2.4	8.8.8.8	0x21a9	Standard query (0)	cdn.rlets.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.590354919 CEST	192.168.2.4	8.8.8.8	0x4601	Standard query (0)	pixel.mathtag.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.612838984 CEST	192.168.2.4	8.8.8.8	0xf643	Standard query (0)	tag.simpli.fi	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.701581001 CEST	192.168.2.4	8.8.8.8	0x29fa	Standard query (0)	apps.twinesocial.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.106021881 CEST	192.168.2.4	8.8.8.8	0x7a85	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.581445932 CEST	192.168.2.4	8.8.8.8	0x3d77	Standard query (0)	61870c77-2e72-45dc-9f17-2f74952d866e.rlets.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.824830055 CEST	192.168.2.4	8.8.8.8	0xe0f9	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.886126995 CEST	192.168.2.4	8.8.8.8	0xa7d5	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.265011072 CEST	192.168.2.4	8.8.8.8	0xf01f	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.561399937 CEST	192.168.2.4	8.8.8.8	0xe30	Standard query (0)	capture-api.reachlocalservices.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.471178055 CEST	192.168.2.4	8.8.8.8	0xb895	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.544157028 CEST	192.168.2.4	8.8.8.8	0xd20b	Standard query (0)	a.adroll.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.736361980 CEST	192.168.2.4	8.8.8.8	0x2cf3	Standard query (0)	apps-cdn.twinesocial.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.774674892 CEST	192.168.2.4	8.8.8.8	0x6ca0	Standard query (0)	s.adroll.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.783866882 CEST	192.168.2.4	8.8.8.8	0x13af	Standard query (0)	d.adroll.mgr.consensu.org	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.897373915 CEST	192.168.2.4	8.8.8.8	0x97a2	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:05.146281004 CEST	192.168.2.4	8.8.8.8	0xc361	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.776218891 CEST	192.168.2.4	8.8.8.8	0x2553	Standard query (0)	ws.pusherapp.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.782813072 CEST	192.168.2.4	8.8.8.8	0xbb95	Standard query (0)	liqadprdct-capture-prod-east.gannettdigital.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.870280981 CEST	192.168.2.4	8.8.8.8	0x8281	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.870801926 CEST	192.168.2.4	8.8.8.8	0x9628	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:47:06.870924950 CEST	192.168.2.4	8.8.8.8	0x5f46	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.871121883 CEST	192.168.2.4	8.8.8.8	0x9f78	Standard query (0)	sync.outbrain.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.871216059 CEST	192.168.2.4	8.8.8.8	0xfd1a	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.472870111 CEST	192.168.2.4	8.8.8.8	0xe5b2	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.472918987 CEST	192.168.2.4	8.8.8.8	0x5949	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.473206043 CEST	192.168.2.4	8.8.8.8	0x199d	Standard query (0)	sync.taboola.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.476049900 CEST	192.168.2.4	8.8.8.8	0xff82	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.476166010 CEST	192.168.2.4	8.8.8.8	0x249a	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.478183985 CEST	192.168.2.4	8.8.8.8	0xd017	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.478564978 CEST	192.168.2.4	8.8.8.8	0xca28	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.494290113 CEST	192.168.2.4	8.8.8.8	0x9555	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.811995983 CEST	192.168.2.4	8.8.8.8	0x7b7c	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.113224030 CEST	192.168.2.4	8.8.8.8	0xabbb	Standard query (0)	graph.facebook.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.114881039 CEST	192.168.2.4	8.8.8.8	0xc4db	Standard query (0)	scontent-iad3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.246710062 CEST	192.168.2.4	8.8.8.8	0x14bc	Standard query (0)	stats.pusher.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.329138994 CEST	192.168.2.4	8.8.8.8	0x5de2	Standard query (0)	scontent-iad3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.330053091 CEST	192.168.2.4	8.8.8.8	0x7c6a	Standard query (0)	scontent-dfw5-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.352945089 CEST	192.168.2.4	8.8.8.8	0xfc4a	Standard query (0)	external-iad3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.378187895 CEST	192.168.2.4	8.8.8.8	0x399c	Standard query (0)	scontent-ort2-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.383299112 CEST	192.168.2.4	8.8.8.8	0xc948	Standard query (0)	scontent-bos3-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.431109905 CEST	192.168.2.4	8.8.8.8	0x9fd2	Standard query (0)	scontent-mia3-2.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.443670034 CEST	192.168.2.4	8.8.8.8	0xb68d	Standard query (0)	scontent-frx5-1.xx.fbcdn.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:17.368731976 CEST	192.168.2.4	8.8.8.8	0xfb3e	Standard query (0)	www.casella.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:21.056521893 CEST	192.168.2.4	8.8.8.8	0x8838	Standard query (0)	secure3.i-doxs.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:24.805640936 CEST	192.168.2.4	8.8.8.8	0x329e	Standard query (0)	ir.casella.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:25.125138998 CEST	192.168.2.4	8.8.8.8	0x9613	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.070106983 CEST	192.168.2.4	8.8.8.8	0x5719	Standard query (0)	api.nasdaqomx.wallst.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.079638004 CEST	192.168.2.4	8.8.8.8	0x40d0	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.750679970 CEST	192.168.2.4	8.8.8.8	0x168f	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.049813986 CEST	192.168.2.4	8.8.8.8	0xbd6c	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.052820921 CEST	192.168.2.4	8.8.8.8	0xd1b1	Standard query (0)	thenasdaqomxgroup.demdex.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.502635002 CEST	192.168.2.4	8.8.8.8	0x537f	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:28.166872978 CEST	192.168.2.4	8.8.8.8	0x2c0c	Standard query (0)	careers-casella.icims.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:28.543668985 CEST	192.168.2.4	8.8.8.8	0x5a63	Standard query (0)	c-11158-20201221-www-casella-com.i.icims.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:28.694250107 CEST	192.168.2.4	8.8.8.8	0x44cd	Standard query (0)	cdn07.icims.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:28.777981043 CEST	192.168.2.4	8.8.8.8	0x4394	Standard query (0)	i.simpli.fi	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:47:29.536402941 CEST	192.168.2.4	8.8.8.8	0xa256	Standard query (0)	s.go-mpulse.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:30.251200914 CEST	192.168.2.4	8.8.8.8	0x3f04	Standard query (0)	c.go-mpulse.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.799417019 CEST	192.168.2.4	8.8.8.8	0x44c8	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.809319973 CEST	192.168.2.4	8.8.8.8	0x9f35	Standard query (0)	stags.bluekai.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.824485064 CEST	192.168.2.4	8.8.8.8	0xe4d6	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.828211069 CEST	192.168.2.4	8.8.8.8	0xe6a7	Standard query (0)	ads.stickyadstv.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.828994036 CEST	192.168.2.4	8.8.8.8	0xb683	Standard query (0)	sync.go.sonobi.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.839243889 CEST	192.168.2.4	8.8.8.8	0xf3f4	Standard query (0)	ce.lijit.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.855200052 CEST	192.168.2.4	8.8.8.8	0x675f	Standard query (0)	uip.semasio.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.863012075 CEST	192.168.2.4	8.8.8.8	0x855f	Standard query (0)	rtb-csync.smartadserver.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.876983881 CEST	192.168.2.4	8.8.8.8	0xf57c	Standard query (0)	sync.search.spotxchange.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.903517008 CEST	192.168.2.4	8.8.8.8	0xca33	Standard query (0)	ads.betweendigital.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.908188105 CEST	192.168.2.4	8.8.8.8	0x3c39	Standard query (0)	mwzeom.zeotap.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.919059038 CEST	192.168.2.4	8.8.8.8	0x7a11	Standard query (0)	loadm.exelator.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.919222116 CEST	192.168.2.4	8.8.8.8	0x17fb	Standard query (0)	ih.adscale.de	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.943698883 CEST	192.168.2.4	8.8.8.8	0x2966	Standard query (0)	ad.sxp.smartclip.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.949079990 CEST	192.168.2.4	8.8.8.8	0x9284	Standard query (0)	su.addthis.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.951380968 CEST	192.168.2.4	8.8.8.8	0x4dcc	Standard query (0)	beacon.krxd.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.972047091 CEST	192.168.2.4	8.8.8.8	0x58f3	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.057329893 CEST	192.168.2.4	8.8.8.8	0x6a53	Standard query (0)	i.liadm.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.071065903 CEST	192.168.2.4	8.8.8.8	0xdd5c	Standard query (0)	sync.crwdcntrl.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.103681087 CEST	192.168.2.4	8.8.8.8	0xda9e	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.106689930 CEST	192.168.2.4	8.8.8.8	0xd068	Standard query (0)	id5-sync.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.309973001 CEST	192.168.2.4	8.8.8.8	0x74aa	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.415992022 CEST	192.168.2.4	8.8.8.8	0xa49c	Standard query (0)	d.agkn.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.475191116 CEST	192.168.2.4	8.8.8.8	0x650e	Standard query (0)	ice.360yield.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.767616987 CEST	192.168.2.4	8.8.8.8	0x1abc	Standard query (0)	i6.liadm.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.923906088 CEST	192.168.2.4	8.8.8.8	0x27c9	Standard query (0)	ads.creative-serving.com	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.212680101 CEST	192.168.2.4	8.8.8.8	0xa5ce	Standard query (0)	uipglob.semasio.net	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.612819910 CEST	192.168.2.4	8.8.8.8	0x1e59	Standard query (0)	rtd-tm.everesttech.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:00.127500057 CEST	8.8.8.8	192.168.2.4	0xe6a9	No error (0)	www.casella.com		52.87.65.167	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.649588108 CEST	8.8.8.8	192.168.2.4	0x4601	No error (0)	pixel.mathtag.com	pixel.mathtag.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:00.672338963 CEST	8.8.8.8	192.168.2.4	0x21a9	No error (0)	cdn.rlets.com	d3bi9sbave64gz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:00.672338963 CEST	8.8.8.8	192.168.2.4	0x21a9	No error (0)	d3bi9sbave64gz.cloudfront.net		65.9.66.129	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.672338963 CEST	8.8.8.8	192.168.2.4	0x21a9	No error (0)	d3bi9sbave64gz.cloudfront.net		65.9.66.58	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.672338963 CEST	8.8.8.8	192.168.2.4	0x21a9	No error (0)	d3bi9sbave64gz.cloudfront.net		65.9.66.74	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.672338963 CEST	8.8.8.8	192.168.2.4	0x21a9	No error (0)	d3bi9sbave64gz.cloudfront.net		65.9.66.120	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.675894976 CEST	8.8.8.8	192.168.2.4	0xf643	No error (0)	tag.simpli.fi		169.50.137.179	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.790458918 CEST	8.8.8.8	192.168.2.4	0x29fa	No error (0)	apps.twinesocial.com	awseb-awseb-eghbt6mzdw45-44179265.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:00.790458918 CEST	8.8.8.8	192.168.2.4	0x29fa	No error (0)	awseb-awseb-eghbt6mzdw45-44179265.us-east-1.elb.amazonaws.com		52.0.228.129	A (IP address)	IN (0x0001)
May 4, 2021 21:47:00.790458918 CEST	8.8.8.8	192.168.2.4	0x29fa	No error (0)	awseb-awseb-eghbt6mzdw45-44179265.us-east-1.elb.amazonaws.com		3.216.17.5	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.163095951 CEST	8.8.8.8	192.168.2.4	0x7a85	No error (0)	googleads.g.doubleclick.net		216.58.212.162	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.646836042 CEST	8.8.8.8	192.168.2.4	0x3d77	No error (0)	61870c77-2e72-45dc-9f17-2f74952d866e.rlets.com		52.88.192.45	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.646836042 CEST	8.8.8.8	192.168.2.4	0x3d77	No error (0)	61870c77-2e72-45dc-9f17-2f74952d866e.rlets.com		52.24.66.224	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.881665945 CEST	8.8.8.8	192.168.2.4	0xe0f9	No error (0)	www.google.de		142.250.185.227	A (IP address)	IN (0x0001)
May 4, 2021 21:47:02.947521925 CEST	8.8.8.8	192.168.2.4	0xa7d5	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:02.947521925 CEST	8.8.8.8	192.168.2.4	0xa7d5	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.316596031 CEST	8.8.8.8	192.168.2.4	0xf01f	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:03.316596031 CEST	8.8.8.8	192.168.2.4	0xf01f	No error (0)	stats.l.doubleclick.net		74.125.133.154	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.316596031 CEST	8.8.8.8	192.168.2.4	0xf01f	No error (0)	stats.l.doubleclick.net		74.125.133.156	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.316596031 CEST	8.8.8.8	192.168.2.4	0xf01f	No error (0)	stats.l.doubleclick.net		74.125.133.157	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.316596031 CEST	8.8.8.8	192.168.2.4	0xf01f	No error (0)	stats.l.doubleclick.net		74.125.133.155	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.622142076 CEST	8.8.8.8	192.168.2.4	0xe30	No error (0)	capture-api.reachlocalservices.com		99.86.2.69	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.622142076 CEST	8.8.8.8	192.168.2.4	0xe30	No error (0)	capture-api.reachlocalservices.com		99.86.2.73	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.622142076 CEST	8.8.8.8	192.168.2.4	0xe30	No error (0)	capture-api.reachlocalservices.com		99.86.2.17	A (IP address)	IN (0x0001)
May 4, 2021 21:47:03.622142076 CEST	8.8.8.8	192.168.2.4	0xe30	No error (0)	capture-api.reachlocalservices.com		99.86.2.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:04.521476030 CEST	8.8.8.8	192.168.2.4	0xb895	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:04.622266054 CEST	8.8.8.8	192.168.2.4	0xd20b	No error (0)	a.adroll.com	a.adroll.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:04.815541029 CEST	8.8.8.8	192.168.2.4	0x2cf3	No error (0)	apps-cdn.twinesocial.com	dyrxq3369g3sr.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:04.815541029 CEST	8.8.8.8	192.168.2.4	0x2cf3	No error (0)	dyrxq3369g3sr.cloudfront.net		65.9.66.12	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.815541029 CEST	8.8.8.8	192.168.2.4	0x2cf3	No error (0)	dyrxq3369g3sr.cloudfront.net		65.9.66.116	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.815541029 CEST	8.8.8.8	192.168.2.4	0x2cf3	No error (0)	dyrxq3369g3sr.cloudfront.net		65.9.66.48	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.815541029 CEST	8.8.8.8	192.168.2.4	0x2cf3	No error (0)	dyrxq3369g3sr.cloudfront.net		65.9.66.84	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.835377932 CEST	8.8.8.8	192.168.2.4	0x6ca0	No error (0)	s.adroll.com	sadroll.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:04.841289043 CEST	8.8.8.8	192.168.2.4	0x13af	No error (0)	d.adroll.mgr.consensu.org	d.adroll.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:04.841289043 CEST	8.8.8.8	192.168.2.4	0x13af	No error (0)	d.adroll.com	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:04.841289043 CEST	8.8.8.8	192.168.2.4	0x13af	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		52.215.226.121	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.841289043 CEST	8.8.8.8	192.168.2.4	0x13af	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		3.248.28.111	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.945970058 CEST	8.8.8.8	192.168.2.4	0x97a2	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.945970058 CEST	8.8.8.8	192.168.2.4	0x97a2	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.945970058 CEST	8.8.8.8	192.168.2.4	0x97a2	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
May 4, 2021 21:47:04.945970058 CEST	8.8.8.8	192.168.2.4	0x97a2	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
May 4, 2021 21:47:05.217474937 CEST	8.8.8.8	192.168.2.4	0xc361	No error (0)	d.adroll.com	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:05.217474937 CEST	8.8.8.8	192.168.2.4	0xc361	No error (0)	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		54.78.31.47	A (IP address)	IN (0x0001)
May 4, 2021 21:47:05.217474937 CEST	8.8.8.8	192.168.2.4	0xc361	No error (0)	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		54.74.23.153	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	ws.pusherapp.com	ws-mt1.pusher.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	ws-mt1.pusher.com	mt1-ws-1895636413.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-1895636413.us-east-1.elb.amazonaws.com		3.208.175.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		52.20.28.166	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		3.222.249.116	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		52.44.236.26	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		100.24.155.60	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		52.205.213.135	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		52.23.0.251	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.828888893 CEST	8.8.8.8	192.168.2.4	0x2553	No error (0)	mt1-ws-189 5636413.us-east-1.el b.amazonaw s.com		107.20.105.92	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.845320940 CEST	8.8.8.8	192.168.2.4	0xbb95	No error (0)	liqadprdct-capture-prod-east.gannettdigital.com	envoy-public.liqadprdct-capture-production-us-east1.gke-eric-eyre-svc.gannettdigital.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.845320940 CEST	8.8.8.8	192.168.2.4	0xbb95	No error (0)	envoy-publ ic.liqadprdct-capture-producti on-us-east1.gke-eric-eyre-svc. gannettdig ital.com		34.75.237.118	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919132948 CEST	8.8.8.8	192.168.2.4	0x8281	No error (0)	simage2.pu bmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.919132948 CEST	8.8.8.8	192.168.2.4	0x8281	No error (0)	pug22000nf c.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.919132948 CEST	8.8.8.8	192.168.2.4	0x8281	No error (0)	pug22000nf .pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	pixel.adve rtising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-a dcom.aolp-ds-prd.aws .oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.57.10.248	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.254.214	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.106.231	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.28.101	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.63.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.153.186	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.99.6	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919375896 CEST	8.8.8.8	192.168.2.4	0x5f46	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.102.119	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.919523954 CEST	8.8.8.8	192.168.2.4	0x9f78	No error (0)	sync.outbrain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.919523954 CEST	8.8.8.8	192.168.2.4	0x9f78	No error (0)	alldcs.outbrain.org	nydc1.outbrain.org		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:06.919523954 CEST	8.8.8.8	192.168.2.4	0x9f78	No error (0)	nydc1.outbrain.org		64.202.112.127	A (IP address)	IN (0x0001)
May 4, 2021 21:47:06.929482937 CEST	8.8.8.8	192.168.2.4	0x9628	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.014250040 CEST	8.8.8.8	192.168.2.4	0xfd1a	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.521699905 CEST	8.8.8.8	192.168.2.4	0x5949	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.521699905 CEST	8.8.8.8	192.168.2.4	0x5949	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.521699905 CEST	8.8.8.8	192.168.2.4	0x5949	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.221.11	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.221.88	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.524616957 CEST	8.8.8.8	192.168.2.4	0x249a	No error (0)	ib.anycast.adnxs.com		185.33.221.52	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	eb2.3lift.com	us-west-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	us-west-eb2.3lift.com	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		3.228.139.221	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		54.236.155.222	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		54.80.39.215	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		18.213.254.247	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		52.200.179.205	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		54.146.205.114	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		54.84.57.130	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.526782990 CEST	8.8.8.8	192.168.2.4	0xd017	No error (0)	dualstack.engagement-bus-prod-713264365.us-east-1.elb.amazonaws.com		34.230.209.57	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.533051014 CEST	8.8.8.8	192.168.2.4	0x199d	No error (0)	sync.taboola.com	am-sync.taboola.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.533051014 CEST	8.8.8.8	192.168.2.4	0x199d	No error (0)	am-sync.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.533051014 CEST	8.8.8.8	192.168.2.4	0x199d	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.537305117 CEST	8.8.8.8	192.168.2.4	0xff82	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.542895079 CEST	8.8.8.8	192.168.2.4	0x9555	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.542895079 CEST	8.8.8.8	192.168.2.4	0x9555	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.543185949 CEST	8.8.8.8	192.168.2.4	0xca28	No error (0)	cm.g.doubleclick.net		142.250.185.162	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		18.195.73.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.158.9.168	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.59.128.17	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.58.55.232	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.156.143.112	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.157.168.25	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		3.124.251.221	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.553245068 CEST	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.28.82.26	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.862582922 CEST	8.8.8.8	192.168.2.4	0x7b7c	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.862582922 CEST	8.8.8.8	192.168.2.4	0x7b7c	No error (0)	prod.ups-ats.aolp-ds-prd.aws.oath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:07.862582922 CEST	8.8.8.8	192.168.2.4	0x7b7c	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
May 4, 2021 21:47:07.862582922 CEST	8.8.8.8	192.168.2.4	0x7b7c	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.170245886 CEST	8.8.8.8	192.168.2.4	0xabbb	No error (0)	graph.facebook.com	api.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:08.170245886 CEST	8.8.8.8	192.168.2.4	0xabbb	No error (0)	api.facebook.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:08.170245886 CEST	8.8.8.8	192.168.2.4	0xabbb	No error (0)	star.c10r.facebook.com		31.13.92.10	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.173726082 CEST	8.8.8.8	192.168.2.4	0xc4db	No error (0)	scontent-iad3-1.xx.fbcdn.net		31.13.66.19	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.306127071 CEST	8.8.8.8	192.168.2.4	0x14bc	No error (0)	stats.pusher.com	timeline49-clientstats1.pusher.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:08.306127071 CEST	8.8.8.8	192.168.2.4	0x14bc	No error (0)	timeline49-clientstats1.pusher.com	ec2-18-233-7-102.compute-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:08.306127071 CEST	8.8.8.8	192.168.2.4	0x14bc	No error (0)	ec2-18-233-7-102.compute-1.amazonaws.com		18.233.7.102	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.387563944 CEST	8.8.8.8	192.168.2.4	0x5de2	No error (0)	scontent-iad3-2.xx.fbcdn.net		157.240.229.1	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.389131069 CEST	8.8.8.8	192.168.2.4	0x7c6a	No error (0)	scontent-dfw5-1.xx.fbcdn.net		157.240.19.26	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.413079977 CEST	8.8.8.8	192.168.2.4	0xfc4a	No error (0)	external-iad3-1.xx.fbcdn.net	scontent-iad3-1.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:08.413079977 CEST	8.8.8.8	192.168.2.4	0xfc4a	No error (0)	scontent-iad3-1.xx.fbcdn.net		31.13.66.19	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.437108994 CEST	8.8.8.8	192.168.2.4	0x399c	No error (0)	scontent-ort2-2.xx.fbcdn.net		157.240.18.19	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.441335917 CEST	8.8.8.8	192.168.2.4	0xc948	No error (0)	scontent-bos3-1.xx.fbcdn.net		157.240.220.14	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.492016077 CEST	8.8.8.8	192.168.2.4	0x9fd2	No error (0)	scontent-mia3-2.xx.fbcdn.net		157.240.14.19	A (IP address)	IN (0x0001)
May 4, 2021 21:47:08.509032965 CEST	8.8.8.8	192.168.2.4	0xb68d	No error (0)	scontent-frx5-1.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
May 4, 2021 21:47:17.575119972 CEST	8.8.8.8	192.168.2.4	0xfb3e	No error (0)	www.casella.com		52.87.65.167	A (IP address)	IN (0x0001)
May 4, 2021 21:47:21.121818066 CEST	8.8.8.8	192.168.2.4	0x8838	No error (0)	secure3.i-doxs.net		209.112.4.23	A (IP address)	IN (0x0001)
May 4, 2021 21:47:25.149420023 CEST	8.8.8.8	192.168.2.4	0x329e	No error (0)	ir.casella.com	casellawastesystems.gcs-web.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:25.149420023 CEST	8.8.8.8	192.168.2.4	0x329e	No error (0)	casellawastesystems.gcs-web.com	leapfrog-ssl-15399.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:25.179223061 CEST	8.8.8.8	192.168.2.4	0x9613	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:25.179223061 CEST	8.8.8.8	192.168.2.4	0x9613	No error (0)	pixel-origin.mathtag.com		185.29.133.52	A (IP address)	IN (0x0001)
May 4, 2021 21:47:25.179223061 CEST	8.8.8.8	192.168.2.4	0x9613	No error (0)	pixel-origin.mathtag.com		185.29.135.190	A (IP address)	IN (0x0001)
May 4, 2021 21:47:25.179223061 CEST	8.8.8.8	192.168.2.4	0x9613	No error (0)	pixel-origin.mathtag.com		185.29.133.208	A (IP address)	IN (0x0001)
May 4, 2021 21:47:25.179223061 CEST	8.8.8.8	192.168.2.4	0x9613	No error (0)	pixel-origin.mathtag.com		185.29.135.227	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.141103029 CEST	8.8.8.8	192.168.2.4	0x40d0	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:26.253917933 CEST	8.8.8.8	192.168.2.4	0x5719	No error (0)	api.nasdaqomx.wallst.com		209.234.234.58	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.157.96	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.194.220.26	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.48.201.185	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.51.81.153	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.250.160.147	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.33.31.50	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.120.236	A (IP address)	IN (0x0001)
May 4, 2021 21:47:26.799416065 CEST	8.8.8.8	192.168.2.4	0x168f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.73.77	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	thenasdaqomxgroup.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.210.171.182	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.250.160.147	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.246.133.154	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.251.60.147	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.31.176.223	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.33.31.50	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.252.115.248	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.114224911 CEST	8.8.8.8	192.168.2.4	0xd1b1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.194.220.26	A (IP address)	IN (0x0001)
May 4, 2021 21:47:27.125487089 CEST	8.8.8.8	192.168.2.4	0xbd6c	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:27.562458038 CEST	8.8.8.8	192.168.2.4	0x537f	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:28.254123926 CEST	8.8.8.8	192.168.2.4	0x2c0c	No error (0)	careers-casella.icims.com	wildcard.icims.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:28.607528925 CEST	8.8.8.8	192.168.2.4	0x5a63	No error (0)	c-11158-20201221-www-casella-com.i.icims.com	wildcard.icims.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:28.753602982 CEST	8.8.8.8	192.168.2.4	0x44cd	No error (0)	cdn07.icims.com	wildcard.icims.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:28.836409092 CEST	8.8.8.8	192.168.2.4	0x4394	No error (0)	i.simpli.fi		169.50.137.179	A (IP address)	IN (0x0001)
May 4, 2021 21:47:29.603988886 CEST	8.8.8.8	192.168.2.4	0xa256	No error (0)	s.go-mpulse.net	ip46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:30.310184002 CEST	8.8.8.8	192.168.2.4	0x3f04	No error (0)	c.go-mpulse.net	wildcard46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:33.848016024 CEST	8.8.8.8	192.168.2.4	0x44c8	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.848016024 CEST	8.8.8.8	192.168.2.4	0x44c8	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.868005991 CEST	8.8.8.8	192.168.2.4	0x9f35	No error (0)	stags.bluekai.com	tags.bluekai.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.877723932 CEST	8.8.8.8	192.168.2.4	0xb683	No error (0)	sync.go.sonobi.com	ams-1-sync.go.sonobi.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.877723932 CEST	8.8.8.8	192.168.2.4	0xb683	No error (0)	ams-1-sync.go.sonobi.com		178.162.133.149	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.887022018 CEST	8.8.8.8	192.168.2.4	0xe4d6	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.887732029 CEST	8.8.8.8	192.168.2.4	0xf3f4	No error (0)	ce.lijit.com	vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.887732029 CEST	8.8.8.8	192.168.2.4	0xf3f4	No error (0)	vap.lijit.com	naw.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.887732029 CEST	8.8.8.8	192.168.2.4	0xf3f4	No error (0)	naw.vap.lijit.com		63.251.14.14	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.887732029 CEST	8.8.8.8	192.168.2.4	0xf3f4	No error (0)	naw.vap.lijit.com		63.251.14.3	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.887732029 CEST	8.8.8.8	192.168.2.4	0xf3f4	No error (0)	naw.vap.lijit.com		209.191.163.209	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.897351980 CEST	8.8.8.8	192.168.2.4	0xe6a7	No error (0)	ads.stickyadstv.com	ip1.ads.stickyadstv.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.906697989 CEST	8.8.8.8	192.168.2.4	0x675f	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.922898054 CEST	8.8.8.8	192.168.2.4	0x855f	No error (0)	rtb-csync.smartadserver.com	2-01-275d-002d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.922898054 CEST	8.8.8.8	192.168.2.4	0x855f	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.89	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.922898054 CEST	8.8.8.8	192.168.2.4	0x855f	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.115	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.922898054 CEST	8.8.8.8	192.168.2.4	0x855f	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.114	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.922898054 CEST	8.8.8.8	192.168.2.4	0x855f	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.113	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.925658941 CEST	8.8.8.8	192.168.2.4	0xf57c	No error (0)	sync.search.spotxchange.com	sync.search-gtm.spotxchange.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.925658941 CEST	8.8.8.8	192.168.2.4	0xf57c	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.125	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.925658941 CEST	8.8.8.8	192.168.2.4	0xf57c	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.126	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.952184916 CEST	8.8.8.8	192.168.2.4	0xca33	No error (0)	ads.betweendigital.com	ssp.ads.betweendigital.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.952184916 CEST	8.8.8.8	192.168.2.4	0xca33	No error (0)	ssp.ads.betweendigital.com		96.46.186.57	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.952184916 CEST	8.8.8.8	192.168.2.4	0xca33	No error (0)	ssp.ads.betweendigital.com		96.46.183.20	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.970755100 CEST	8.8.8.8	192.168.2.4	0x17fb	No error (0)	ih.adscale.de		18.197.81.144	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.970755100 CEST	8.8.8.8	192.168.2.4	0x17fb	No error (0)	ih.adscale.de		18.158.173.146	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:33.970755100 CEST	8.8.8.8	192.168.2.4	0x17fb	No error (0)	ih.adscale.de		3.123.78.164	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.971723080 CEST	8.8.8.8	192.168.2.4	0x3c39	No error (0)	mwzeom.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.971723080 CEST	8.8.8.8	192.168.2.4	0x3c39	No error (0)	mwzeom.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.971723080 CEST	8.8.8.8	192.168.2.4	0x3c39	No error (0)	mwzeom.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.977993011 CEST	8.8.8.8	192.168.2.4	0x7a11	No error (0)	loadm.exelator.com	loadus.tm.ssl.exelator.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.977993011 CEST	8.8.8.8	192.168.2.4	0x7a11	No error (0)	loadus.tm.ssl.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.977993011 CEST	8.8.8.8	192.168.2.4	0x7a11	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:33.977993011 CEST	8.8.8.8	192.168.2.4	0x7a11	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		34.252.166.236	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		52.48.138.155	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		54.228.50.17	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		108.128.72.76	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		52.19.39.131	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		52.215.165.29	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		52.17.174.227	A (IP address)	IN (0x0001)
May 4, 2021 21:47:33.995016098 CEST	8.8.8.8	192.168.2.4	0x2966	No error (0)	ad.sxp.smartclip.net		52.17.244.53	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	beacon.krxd.net	beacon-dub-prod.krxd.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	beacon-dub-prod.krxd.net	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.246.207.243	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.170.10.95	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.252.41.130	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.49.95.65	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.48.21.41	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		63.35.129.75	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.48.82.49	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.000679970 CEST	8.8.8.8	192.168.2.4	0x4dcc	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.255.31.14	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.013077021 CEST	8.8.8.8	192.168.2.4	0x9284	No error (0)	su.addthis.com	m.addthisedge.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.013077021 CEST	8.8.8.8	192.168.2.4	0x9284	No error (0)	m.addthisedge.com	ds-m.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.043961048 CEST	8.8.8.8	192.168.2.4	0x58f3	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	i.liadm.com	idaas-ext.cph.liveintent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		54.81.208.30	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		54.209.231.92	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		52.205.241.172	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		54.81.204.200	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		52.73.155.220	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		52.86.51.18	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		52.55.124.30	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.117476940 CEST	8.8.8.8	192.168.2.4	0x6a53	No error (0)	idaas-ext.cph.liveintent.com		54.82.140.152	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		54.194.226.253	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		34.251.130.56	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		54.171.173.220	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		52.208.103.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		34.253.111.115	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.133951902 CEST	8.8.8.8	192.168.2.4	0xdd5c	No error (0)	sync.crwdcntrl.net		52.30.14.23	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa.agkn.com	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		35.176.232.241	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.132.239.61	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.133.35.94	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		52.56.207.211	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		52.56.111.113	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.155416965 CEST	8.8.8.8	192.168.2.4	0xda9e	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.11.29.5	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match.adsrvr.org	match-243508202.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		44.241.59.199	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		54.186.22.124	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		52.25.20.110	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		54.148.24.135	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		52.41.50.195	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		44.239.245.89	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		52.43.153.20	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.358489990 CEST	8.8.8.8	192.168.2.4	0x74aa	No error (0)	match-243508202.us-west-2.elb.amazonaws.com		100.20.9.202	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	d.agkn.com	data.agkn.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	data.agkn.com	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		52.28.108.245	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.194.113.221	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.195.77.77	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		52.29.48.214	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.196.98.222	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.480756998 CEST	8.8.8.8	192.168.2.4	0xa49c	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.195.194.125	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	ice.360yield.com	eu2-ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		52.58.206.142	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		52.28.69.126	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		52.57.77.12	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		52.57.228.122	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		54.93.141.230	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		52.57.243.4	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		54.93.160.53	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.537678003 CEST	8.8.8.8	192.168.2.4	0x650e	No error (0)	eu2-ice.360yield.com		18.158.182.200	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	i6.liadm.com	idaas6.cph.liveintent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		3.209.93.152	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		34.202.20.24	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		52.70.165.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		52.73.168.142	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		52.20.143.54	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		34.231.219.220	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		34.198.52.7	A (IP address)	IN (0x0001)
May 4, 2021 21:47:34.819392920 CEST	8.8.8.8	192.168.2.4	0x1abc	No error (0)	idaas6.cph.liveintent.com		34.202.24.13	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.072402000 CEST	8.8.8.8	192.168.2.4	0x27c9	No error (0)	ads.creative-serving.com	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:35.072402000 CEST	8.8.8.8	192.168.2.4	0x27c9	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.123.96.39	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.072402000 CEST	8.8.8.8	192.168.2.4	0x27c9	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		18.185.0.221	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.072402000 CEST	8.8.8.8	192.168.2.4	0x27c9	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.127.51.194	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.072402000 CEST	8.8.8.8	192.168.2.4	0x27c9	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		18.158.167.137	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.269735098 CEST	8.8.8.8	192.168.2.4	0xa5ce	No error (0)	uipglob.semasio.net	uipglob.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:35.269735098 CEST	8.8.8.8	192.168.2.4	0xa5ce	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)
May 4, 2021 21:47:35.672290087 CEST	8.8.8.8	192.168.2.4	0x1e59	No error (0)	rtd-tm.everesttech.net	rtd.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:47:35.672290087 CEST	8.8.8.8	192.168.2.4	0x1e59	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.casella.com
  - cdn.rlets.com
  - apps.twinesocial.com
    - apps-cdn.twinesocial.com
    - stats.pusher.com
  - connect.facebook.net
- ws.pusherapp.com

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5488 Parent PID: 800

General

Start time:	21:46:57
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff619a50000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Copyright Joe Security LLC 2021

Analysis Process: iexplore.exe PID: 5840 Parent PID: 5488

General

Start time:	21:46:58
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5488 CREDAT:17410 /prefetch:2
Imagebase:	0xbc0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Copyright Joe Security LLC 2021