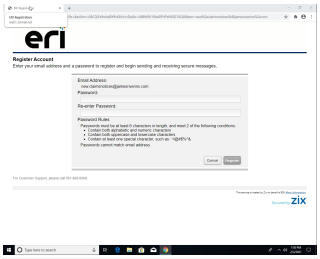
ID: 348203
Cookbook: browseurl.jbs
Time: 19:49:09
Date: 03/02/2021
Version: 31.0.0 Emerald

Table of Contents

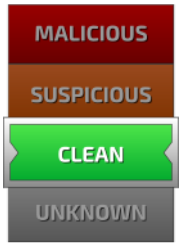
Analysis Report https://web1.zixmail.net/s/e?b=4eri&m=…

Overview

General Information

Sample URL:	http://https://web1.zixmail.net/s/e?b=4eri&m=ABCQiFe9wlqI9X9vKBvYvvDp&c=ABBhRV19Ad0FHPsNXID7AQI6&em=new.claimsnotices%40jamesriverins.com
Analysis ID:	348203
Most interesting Screenshot:	

Detection



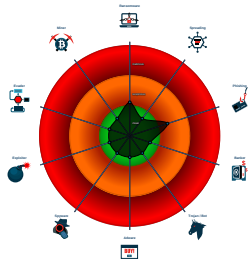
Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

HTML body contains low number of …

HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6956 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://web1.zixmail.net/s/e?b=4eri&m=ABCQiFe9wlqI9X9vKBvYvvDp&c=ABBhRV19Ad0FHPsNXID7AQI6&em=new%2eclaimsnotices%40jamesriverins%2ecom' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7128 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,991956672690595382,7383702837834195658,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6460 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1552,991956672690595382,7383702837834195658,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=2192 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

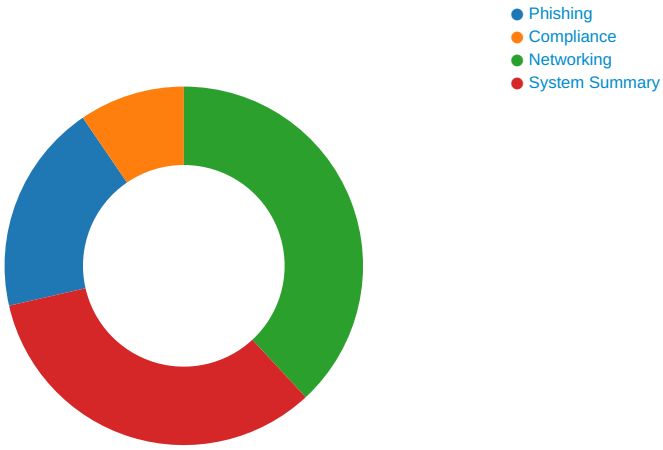
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

Compliance:

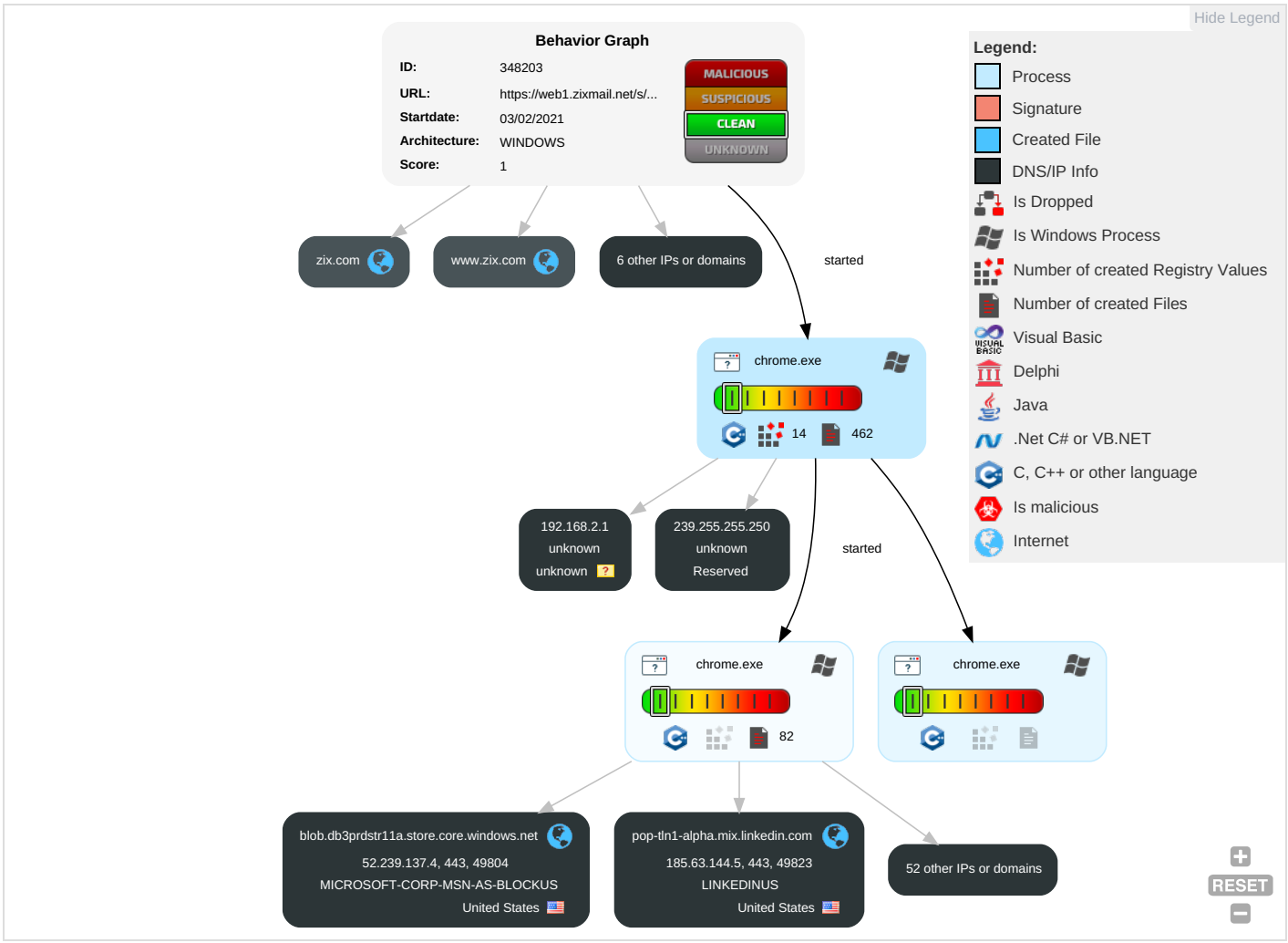
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 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

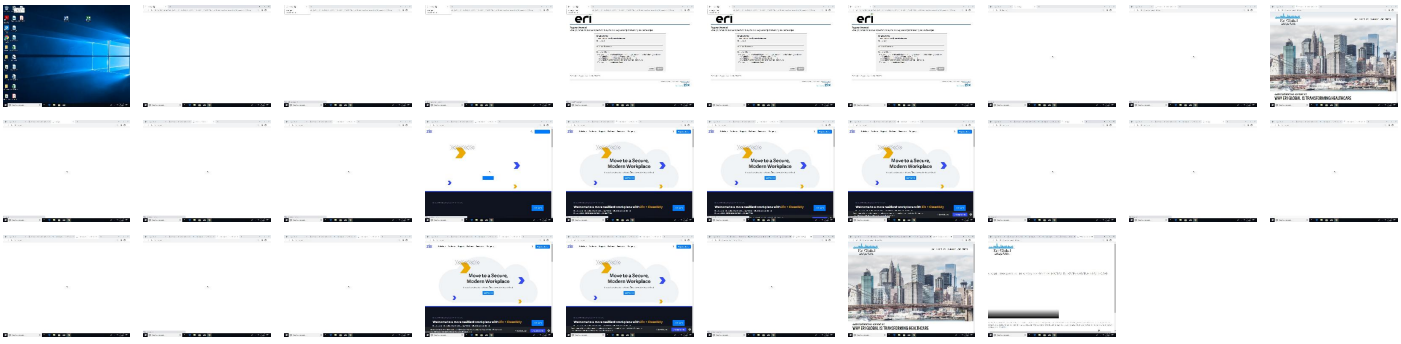
Behavior Graph

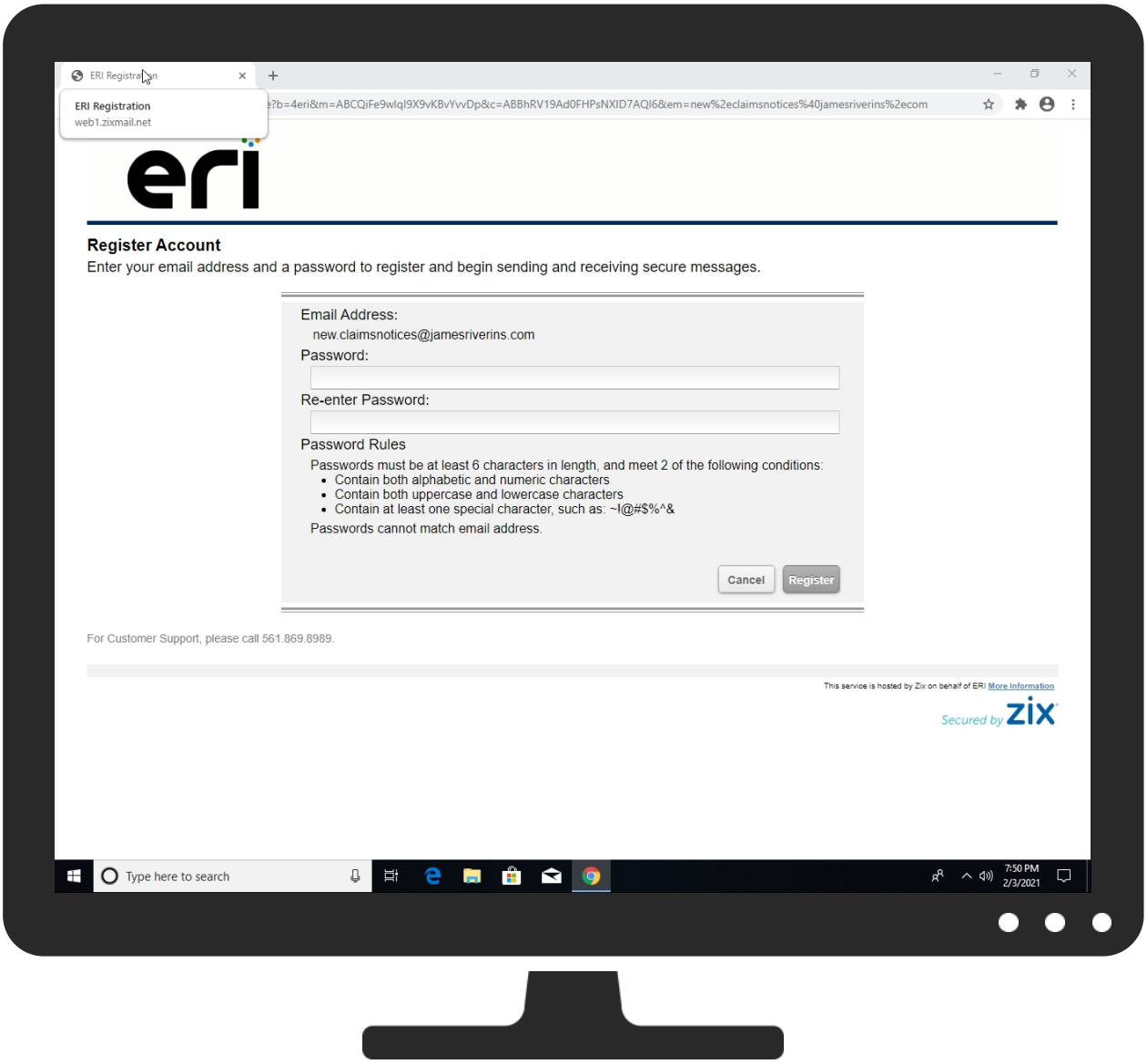


Screenshots

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://https://web1.zixmail.net/s/e?b=4eri&m=ABCQiFe9wlqI9X9vKBvYvvDp&c=ABBhRV19Ad0FHPsNXID7AQI6&em=new%2eclaimsnotices%40jamesriverins%2ecom	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
4eri.com	0%	Virustotal		Browse
segments.company-target.com	0%	Virustotal		Browse
eriglobal.com	0%	Virustotal		Browse
match.prod.bidr.io	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://zix.com//	0%	Avira URL Cloud	safe	
http://eriglobal.com/css/fonts/oswald-regular.woff2	0%	Avira URL Cloud	safe	
http://eriglobal.com/8	0%	Avira URL Cloud	safe	
http://https://zix.com/2	0%	Avira URL Cloud	safe	
http://https://zix.com/4	0%	Avira URL Cloud	safe	
http://https://zix.comh	0%	Avira URL Cloud	safe	
http://eriglobal.com/js/default.js	0%	Avira URL Cloud	safe	
http://https://www.zix.com/core/misc/drupal.js?v=8.9.10	0%	Avira URL Cloud	safe	
http://eriglobal.com/css/fonts/opensans-semibold.woff	0%	Avira URL Cloud	safe	
http://https://zix.com/themes/custom/zix/favicon.ico	0%	Avira URL Cloud	safe	
http://eriglobal.com/css/plugins/alerts.css	0%	Avira URL Cloud	safe	
http://https://customer2.api.driftqa.com	0%	Avira URL Cloud	safe	
http://https://conversation2.api.driftqa.com	0%	Avira URL Cloud	safe	
http://https://identify.api.driftqa.com	0%	Avira URL Cloud	safe	
http://https://zix.com/l	0%	Avira URL Cloud	safe	
http://https://zix.com/libraries/bootstrap/dist/js/bootstrap.js?v=1.x	0%	Avira URL Cloud	safe	
http://https://metrics.api.driftqa.com	0%	Avira URL Cloud	safe	
http://eriglobal.com/uploads/videos/c4ca4238a0b923820dcc509a6f75849b/videoplayback-1558705888.mp4	0%	Avira URL Cloud	safe	
http://https://www.zix.com	0%	Avira URL Cloud	safe	
http://https://enrichment.api.driftqa.com	0%	Avira URL Cloud	safe	
http://ocsp.affirmtrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRtMhZQYpqo2xxcFXSxtJGrbVcLygQU2%2B9lNwvlR8	0%	Avira URL Cloud	safe	
http://https://messaging.api.driftqa.com	0%	Avira URL Cloud	safe	
http://https://www.zix.com/core/assets/vendor/jquery/jquery.min.js?v=3.5.1	0%	Avira URL Cloud	safe	
http://eriglobal.com/images/b-bullet.png	0%	Avira URL Cloud	safe	
http://eriglobal.com/#topp	0%	Avira URL Cloud	safe	
http://eriglobal.com/css/plugins/bt.css	0%	Avira URL Cloud	safe	
http://eriglobal.com/images/build3.jpg	0%	Avira URL Cloud	safe	
http://https://embeds.driftcdn.com	0%	Avira URL Cloud	safe	
http://https://zix.com/themes/custom/zixappriver/js/main.js?v=1.x	0%	Avira URL Cloud	safe	
http://https://www.zix.com/search	0%	Avira URL Cloud	safe	
http://https://targeting.api.driftqa.com	0%	Avira URL Cloud	safe	
http://https://zix.com/Y	0%	Avira URL Cloud	safe	
http://https://zix.com/B&s	0%	Avira URL Cloud	safe	
http://eriglobal.com/images/bull.jpg	0%	Avira URL Cloud	safe	
http://https://meetings.api.driftqa.com	0%	Avira URL Cloud	safe	
http://https://zix.com/Email	0%	Avira URL Cloud	safe	
http://https://www.zix.com/t	0%	Avira URL Cloud	safe	
http://https://www.zix.com/themes/custom/zix/favicon.ico/	0%	Avira URL Cloud	safe	
http://eriglobal.com/images/bottom-BG2.jpg	0%	Avira URL Cloud	safe	
http://https://zix.com//Email	0%	Avira URL Cloud	safe	
http://eriglobal.com/images/cuild2.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alb-event-1454785217.us-east-1.elb.amazonaws.com	18.205.49.143	true	false		high
4eri.com	184.168.131.241	true	false	• 0%, Virustotal, Browse	unknown
www.zixcorp.com	199.30.234.249	true	false		high
afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com	54.147.21.139	true	false		high
segments.company-target.com	99.86.167.90	true	false	• 0%, Virustotal, Browse	unknown
ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	54.198.218.148	true	false		high
eriglobal.com	68.233.236.236	true	false	• 0%, Virustotal, Browse	unknown
dl7g9llrghqi1.cloudfront.net	143.204.2.71	true	false		high
tag.demandbase.com	143.204.2.74	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	54.85.240.191	true	false		high
www.webdesignerexpress.com	172.67.138.15	true	false		high
z-p42-instagram.c10r.facebook.com	185.60.216.174	true	false		high
id.rlcdn.com	34.120.207.148	true	false		high
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
twitter.com	104.244.42.129	true	false		high
match.prod.bidr.io	54.72.203.0	true	false	• 0%, Virustotal, Browse	unknown
js.driftqa.com	3.229.202.186	true	false		unknown
stats.l.doubleclick.net	108.177.15.156	true	false		high
targeting.api.drift.com	100.24.186.63	true	false		high
zix.com	199.30.234.249	true	false		unknown
www.zix.com	199.30.234.249	true	false		unknown
embeds.driftcdn.com	13.226.169.56	true	false		unknown
pop-tln1-alpha.mix.linkedin.com	185.63.144.5	true	false		high
bootstrap.api.drift.com	18.215.11.20	true	false		high
web1.zixmail.net	63.71.15.50	true	false		high
www.bugherd.com.herokudns.com	3.213.190.117	true	false		unknown
blob.db3prdstr11a.store.core.windows.net	52.239.137.4	true	false		high
api.company-target.com	99.86.167.33	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.20.225	true	false		high
presence.api.drift.com	unknown	unknown	false		high
metrics.api.drift.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
js.driftt.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
customer.api.drift.com	unknown	unknown	false		high
event.api.drift.com	unknown	unknown	false		high
www.bugherd.com	unknown	unknown	false		high
conversation.api.drift.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
115079-29.chat.api.drift.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
optanon.blob.core.windows.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
ocsp.affirmtrust.com	unknown	unknown	false		unknown
www.instagram.com	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
ocsp.entrust.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://eriglobal.com/css/fonts/oswald-regular.woff2	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/	false		unknown
http://eriglobal.com/js/default.js	false	• Avira URL Cloud: safe	unknown
http://https://zix.com/	false		unknown
http://eriglobal.com/css/fonts/opensans-semibold.woff	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core?embedId=65e63pi6mu5c&forceShow=false&skipCampaigns=false&sessionId=b37c012e-a28c-431b-b8c9-9a6e07b0fca5&sessionStarted=1612410652&campaignRefreshToken=b76b3bc0-4b91-485c-92a0-0bd0bebe41e1&pageLoadStartTime=1612410645525	false		high
http://eriglobal.com/css/plugins/alerts.css	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/chat	false		high
http://eriglobal.com/uploads/videos/c4ca4238a0b923820dcc509a6f75849b/videoplayback-1558705888.mp4	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/images/b-bullet.png	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/css/plugins/bt.css	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/images/build3.jpg	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/images/bull.jpg	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/images/bottom-BG2.jpg	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/images/cuild2.jpg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zix.com//	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/26.91e0f92d.chunk.js	01c430a9b102894d_0.0.dr	false		high
http://https://www.linkedin.com	8a345bb5-7d51-419f-b6fe-6a34e791b7cf.tmp.1.dr	false		high
http://https://js.driftt.com/core/assets/js/13.a9247e5d.chunk.jsaD	3b38794615c80537_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/28.a2bddfe2.chunk.jsaD	2fd021f1c66e0410_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/36.56cefaf3.chunk.js	50283a465e0a4d29_0.0.dr	false		high
http://eriglobal.com/8	7658764de37070f0_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/25.5675afde.chunk.jsaD	efc82e9adcf42c5c_0.0.dr	false		high
http://https://js.driftt.com/core?embedId=65e63pi6mu5c&forceShow=false&skipCampaigns=false&sessionId=ac0f9c	Current Session.0.dr	false		high
http://https://px.ads.linkedin.com/collect?	648f965c0b7dabbc_0.0.dr	false		high
http://https://zix.com/2	f547e4ebb0310f07_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zix.com/4	f547e4ebb0310f07_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zix.comh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/32.24776eab.chunk.js	23aff70ab1c25091_0.0.dr	false		high
http://https://metrics.api.drift.com	c0e42b091147ff06_0.0.dr	false		high
http://https://www.zix.com/core/misc/drupal.js?v=8.9.10	bd3855900f676b3a_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zix.com/	Current Session.0.dr, 2147111f92e1d00b_0.0.dr, 000003.log0.0.dr	false		unknown
http://https://js.driftt.com/core/assets/js/36.56cefaf3.chunk.jsaD	50283a465e0a4d29_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/2.04b0c69b.chunk.js	9b493ae1aa245169_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/43.0bd3f7fc.chunk.jsaD	10cf6fd86d883fb4_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/1.0af467a5.chunk.jsa	484a67f8e93657dc_0.0.dr	false		high
http://https://zix.com/themes/custom/zix/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zixmail.net/S	ca75a81802d989a1_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/19.d206834e.chunk.js	f526fee988bc24e1_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/25.5675afde.chunk.js	efc82e9adcf42c5c_0.0.dr, 9c58a5bd2d855331_0.0.dr	false		high
http://https://customer2.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/0.45eb4005.chunk.jsaD	f7267d924f102f30_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/main~970f9218.06709018.chunk.jsa	b2f66da88d7b43b0_0.0.dr	false		high
http://https://conversation2.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/runtime~main.643a3a55.jsaD	8d86142e4c1aaf72_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/main~53ca99a6.4d7f7a8a.chunk.jsaD	48367205b83f4fa8_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/runtime~main.643a3a55.js	8d86142e4c1aaf72_0.0.dr	false		high
http://https://identify.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zix.com/l	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zix.com/libraries/bootstrap/dist/js/bootstrap.js?v=1.x	05fcd8b85e1b3284_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/23.5562c7f5.chunk.jsaD	0732e770b7a445ab_0.0.dr	false		high
http://https://metrics.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.zix.com	000003.log6.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://enrichment.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.affirmtrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRtMhZQYpqo2xxcFXSxtJGrbVcLygQU2%2B9lNwvlR8	2508E8D974CC05F224A38A6A068698E0_79F9901B6CE1C0907957A8D61937ACE1.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://driftt.com/4tC	8d86142e4c1aaf72_0.0.dr	false		high
http://https://messaging.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.zix.com/core/assets/vendor/jquery/jquery.min.js?v=3.5.1	57e301f7a5008375_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://eriglobal.com/#topp	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zixmail.net/	9bea1099a402aeb8_0.0.dr	false		high
http://https://embeds.driftcdn.com	8a345bb5-7d51-419f-b6fe-6a34e791b7cf.tmp.1.dr, c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBTLXNCzDvBhHecWjg70iJhBW0InywQUanImetAe733nO2lR	A37B8BA80004D3266CB4D93B2052DC10_994B5C515D64A296EABD42B0A2E46349.1.dr	false		high
http://https://js.driftt.com/core/assets/js/38.feef3c6b.chunk.jsaD	00a1982a45dd042c_0.0.dr	false		high
http://https://customer.api.drift.com	c0e42b091147ff06_0.0.dr	false		high
http://https://zix.com/themes/custom/zixappriver/js/main.js?v=1.x	8164647a8748d80a_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://integration.drift.com	c0e42b091147ff06_0.0.dr	false		high
http://https://www.zix.com/search	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/14.274c57c3.chunk.jsaD	03ca1713717c7b03_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/main~493df0b3.1bfc4c5f.chunk.js	c0e42b091147ff06_0.0.dr	false		high
http://https://targeting.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://zix.com/Y	deeb90394251543d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/17.0833007f.chunk.jsaD	20649622586617ff_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/38.feef3c6b.chunk.js	00a1982a45dd042c_0.0.dr	false		high
http://https://use.typekit.net	8a345bb5-7d51-419f-b6fe-6a34e791b7cf.tmp.1.dr	false		high
http://https://js.driftt.com/core/assets/js/20.ec5afb3b.chunk.jsaD	f2c5b710fbc9e04f_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/main~2e35577e.69c90f86.chunk.js	36211ac3aab3f4f0_0.0.dr	false		high
http://https://zix.com/B&s	f2d69cb8ea7d653f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.giphy.com/v1/gifs	c0e42b091147ff06_0.0.dr	false		high
http://https://meetings.api.driftqa.com	c0e42b091147ff06_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/15.ba891359.chunk.js	f44589422015 58ca_0.0.dr, 791d5b9834f8c9fd_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/34.fe729046.chunk.js	655aacf938afda06_0.0.dr, 90e0fc941053c5e0_0.0.dr	false		high
http://https://zix.com/Email	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/20.ec5afb3b.chunk.js	f2c5b710fbc9e04f_0.0.dr	false		high
http://https://conversation.api.drift.com	c0e42b091147ff06_0.0.dr	false		high
http://https://web1.zixmail.net/s/REL-5.11.17.280/userNotifier.js	9bea1099a402aeb8_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/35.9da4441f.chunk.jsaD	08d63749a47a6a6d_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/main~53ca99a6.4d7f7a8a.chunk.jsa	48367205b83f4fa8_0.0.dr	false		high
http://https://driftt.com/	36211ac3aab3f4f0_0.0.dr, 03cf3aa0642e3d9a_0.0.dr, 2fd021f1c66e0410_0.0.dr, 11c9e752de6044e2_0.0.dr	false		high
http://ocsp.entrust.net/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQnuEQcScL%2FkljKed%2BRzpzFYOq9kwQUw%2FfQtSowra	D8A5A4A0441F7653C3609E0E2DE6769F_7CB1F9CF5591E73A1593763D843A4B86.1.dr	false		high
http://https://web1.zixmail.net/s/REL-5.11.17.280/emailfieldvalue.js	eadf69b2511119d6_0.0.dr	false		high
http://https://flow.api.drift.com	c0e42b091147ff06_0.0.dr	false		high
http://https://js.driftt.com/core/assets/js/34.fe729046.chunk.jsaD	90e0fc941053c5e0_0.0.dr	false		high
http://https://optanon.blob.core.windows.net/	Network Action Predictor-journal.0.dr	false		high
http://https://web1.zixmail.net/s/e?b=4eri&m=ABCQiFe9wlqI9X9vKBvYvvDp&c=ABBhRV19Ad0FHPsNXID7AQI6&em=new%2ec	History-journal.0.dr	false		high
http://https://www.zix.com/t	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.zix.com/themes/custom/zix/favicon.ico/	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.driftt.com/core/assets/js/12.8c7dd5ee.chunk.js	85eb2726a8e59d21_0.0.dr	false		high
http://https://snap.licdn.com/li.lms-analytics/insight.min.jsaD	648f965c0b7dabbc_0.0.dr	false		high
http://https://zix.com//Email	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.156	unknown	United States		15169	GOOGLEUS	false
63.71.15.50	unknown	United States		13380	ASN-CUSTUS	false
99.86.167.90	unknown	United States		16509	AMAZON-02US	false
18.215.11.20	unknown	United States		14618	AMAZON-AESUS	false
13.226.169.56	unknown	United States		16509	AMAZON-02US	false
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
99.86.167.33	unknown	United States		16509	AMAZON-02US	false
54.147.21.139	unknown	United States		14618	AMAZON-AESUS	false
172.217.20.225	unknown	United States		15169	GOOGLEUS	false
52.239.137.4	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
18.205.49.143	unknown	United States		14618	AMAZON-AESUS	false
185.63.144.5	unknown	United States		14413	LINKEDINUS	false
34.120.207.148	unknown	United States		15169	GOOGLEUS	false
54.85.240.191	unknown	United States		14618	AMAZON-AESUS	false
199.30.234.249	unknown	United States		13380	ASN-CUSTUS	false
143.204.2.74	unknown	United States		16509	AMAZON-02US	false
54.72.203.0	unknown	United States		16509	AMAZON-02US	false
143.204.2.71	unknown	United States		16509	AMAZON-02US	false
54.198.218.148	unknown	United States		14618	AMAZON-AESUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
3.229.202.186	unknown	United States		14618	AMAZON-AESUS	false
100.24.186.63	unknown	United States		14618	AMAZON-AESUS	false
68.233.236.236	unknown	United States		29802	HVC-ASUS	false
3.213.190.117	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	348203
Start date:	03.02.2021
Start time:	19:49:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://web1.zixmail.net/s/e?b=4eri&m=ABCQiFe9wlqI9X9vKBvYvvDp&c=ABBhRV19Ad0FHPsNXID7AQI6&em=new.claimsnotices%40jamesriverins.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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@38/257@46/27
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: http://4eri.com/ • Browse: https://www.zix.com/ • Browse: http://www.zixcorp.com/ • Browse: http://eriglobal.com/#top • Browse: http://eriglobal.com/
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 52.255.188.83, 172.217.22.205, 172.217.23.78, 216.58.207.174, 173.194.187.72, 93.184.221.240, 173.194.151.90, 2.20.16.37, 216.58.207.131, 172.217.22.234, 216.58.207.138, 216.58.207.170, 172.217.20.234, 172.217.23.42, 172.217.23.74, 172.217.22.202, 172.217.23.40, 13.107.42.14, 172.217.23.46, 92.122.213.187, 92.122.213.200, 23.37.33.211, 172.217.23.67, 92.122.254.114, 209.197.3.24, 192.124.249.24, 192.124.249.41, 192.124.249.23, 192.124.249.22, 192.124.249.36, 51.103.5.186, 20.190.137.75, 20.190.137.69, 20.190.137.73, 40.126.9.6, 20.190.137.6, 20.190.137.96, 40.126.9.66, 20.190.137.98, 51.104.139.180, 216.58.207.163, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 92.122.253.206, 74.125.11.104 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, e6653.dscf.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, clientservices.googleapis.com, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, l-0005.l-msedge.net, clients2.google.com, use-stls.adobe.com.edgesuite.net, emea1.wns.notify.trafficmanager.net, login.live.com, r3---sn-4g5e6nzl.gvt1.com, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, r4---sn-4g5e6nez.gvt1.com, watson.telemetry.microsoft.com, www.gstatic.com,

ocsp.godaddy.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, www.googleapis.com, r3.sn-4g5e6nzl.gvt1.com, ocsp.entrust.net.edgekey.net, ris.api.iris.microsoft.com, r3---sn-4g5e6nsk.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, e6913.dscx.akamaiedge.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wu.azureedge.net, arc.msn.com, e9706.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, redirector.gvt1.com, www.googletagmanager.com, cs11.wpc.v0cdn.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, r3.sn-4g5e6nsk.gvt1.com, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, www-linkedin-com.l-0005.l-msedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, p.typekit.net-v3.edgekey.net, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, wu.ec.azureedge.net, www-googletagmanager.l.google.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, r4.sn-4g5e6nez.gvt1.com, login.msa.msidentity.com, skypedataprdcoleus17.cloudapp.net, wildcard.licdn.com.edgekey.net, ocsp.godaddy.com, skypedataprdcolwus16.cloudapp.net, a1988.dscg1.akamai.net

- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:50:01	API Interceptor	8x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0C2A6B05AF7011FB1228AE98D31E7D22_906CFB2450238D0B4C3B6D559BA937CB	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1465
Entropy (8bit):	7.466560278519602
Encrypted:	false
SSDEEP:	24:LcWAAjEKOXGtdKeMBizE9sLVCSiWAAB7DyhkZMdG2BsvmS8uwlKCTxrIGF2S3xSB:RAAoKOkdzFzE9KHAAxuhcMiMuOKCBIGU
MD5:	1BD62D20EE8662F134088F9F6E970B31
SHA1:	4749C2E297B149B2CB3FA65B6E7B8DF8EE41D94B
SHA-256:	FDB32A86522D1F2E3FF6295FF1A00EF088D4F6F3A1682019349F115C84C6971B
SHA-512:	C594AC938C1953A216D9F6DE1BABA59C3CE3731CCB8E287835D8F39B5E0485906F91FA0836D4999F9DC7733629713D104055E302C80F8AC2BF69262983333D4A
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0..P0N1.0...U....US1.0...U....AffirmTrust1)0'..U... AffirmTrust Validation Authority..20210203090900Z0k0i0A0...+.....8...a.9O....V#..u.....S.^.?.....$.....@.....20210203090000Z....20210210090000Z0...*.H.....\..no~.|.+.....G5...%.._.UQwZg.d...s..T.9.am?x..+.....Zc}q#E.!Za..Y8.Se...4...i....y8.....e...i.P..L.....#S.{.*>...j.j./..zy.Nn.V[]..{P.ZV.....(rM..v:.....kq..J...I.....2.].b.Wz...Dd..-...cq.2U'...2...].!..^.\..N.[fG....Ejt.{.Z..;..Z..aE....0...0...0.....WD.....@....b..?0...*.H.....0D1.0...U....US1.0...U....AffirmTrust1.0...U....AffirmTrust Commercial0...200724141959Z..210724141959Z0N1.0...U....US1.0...U....AffirmTrust1)0'..U... AffirmTrust Validation Authority0.."0...*.H.....0.....P.i..xF=a,...=.....Q.k..lu..Q.O.....T.3oN0.....R.x?o.....`<...>.I.y.t.M...G.p.....Q[...G.7.N.Mt.....N..Q..."V#;...d.....!=.`...O<vx.....'.[k..~.)5`...DV.R.^.VRI....K.^JN.Q"..K....DL..!]

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1731
Entropy (8bit):	7.292056503376296
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
SSDEEP:	48:panitqt0Ah7bnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pW57uz1+boavLJpu5
MD5:	D13FC28B2ED31AD5621C624270FB0D74
SHA1:	B646791147C73A77B61E350E932FF830640CF4CA
SHA-256:	315AAE91334CA3D6E1CF6A1A0FA802B1443F6D40CEAE1C8FDDB69418D894AAF0
SHA-512:	C7C892DDB72A7B723A82312DD03C9AB3775B748A7DB01912239E49E022FE8158F78EAE885E5BD903F541658B6A5742185E13B0E621CF30D2EA684885E3533160
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G2..20210202193528Z0d0b0:0...+.....#o..K.....#....+..:....g(.....An .....20210202193528Z....20210204073528Z0...*.H.....| .cY...6.M....&.c..@t.....@..\.....49..x....'_..t.)p5/.:,.J'=O.F;HE....u.l.MD.H1.@{..pO..t9^..g..,.+K.k3]....p.o%%.v...U....f....k..F...A.:...s.....n.Q.E..IVR.me.D.v..'\#$<.....G.(...PE.PF.....i..C.o$....%j.Q|b.TF..%.L.&.6{...}.. ...k4....0...0...0..g.....f...p.t0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...200909070000Z..210909070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G20.."0...*.H.....0.....'.....^Y.u..U.qU..."......-]XG(qk#.+....J...G.3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2508E8D974CC05F224A38A6A068698E0_1FA4F51F50E531077AD3338680850105	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1535
Entropy (8bit):	7.451187680632366
Encrypted:	false
SSDEEP:	24:9WppAIM/bsCGd4LF838eD/uB2JcziQCBdppAB7McNXppDBuxpD4uE4GrRu4L85+W:98pA1okF838eDgZCppAxMu5pDBuxeuam
MD5:	A3EE2287CEA77BB83D7688DAEA37846D
SHA1:	2CE1D02ED1E1C973DF6D89017B3101073095E998
SHA-256:	A7409B74FAE2E7260691523F1D98E966A810BB52DBA835B4413994F76EA232F0
SHA-512:	326CD9DEBBE15AE1232BE4E179CBE89D708FB8CDC7E819EF688840A1467D3B2BBC982865F0E8801C6A76AD7498323F01A1C6DE63135C9D2E154B13BCD0CEDC9
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0..P0N1.0...U....CA1.0...U....AffirmTrust1)0'..U... AffirmTrust Validation Authority..20210203085400Z0s0q0l0...+.....m2.Pb....\.t....mW.....e7..G.5.....:...kH.....X.H....20210203080000Z....20210210080000Z0...*.H.....?`...S..s.6')}.....J.H....j..)./..F=...s.....}Y...{....{...b`hY.w.k..e...$`.....)....D.U=.....:...c..[!...6n..cU..?r...l.....+.e.IJM.fP.7j.K.<x..GQjr....J..IF...}.....Z....?g?..C..G.....3...~.P.69mI...>....@Ob..._....MF`.....0...0...0.....j.+.....X.cs0...*.H.....0..1.0...U....CA1.0...U....AffirmTrust1+0)..U..."See www.affirmtrust.com/repository110/..U...(AffirmTrust Extended Validation CA - EV10...191101190651Z..221101193651Z0N1.0...U....CA1.0...U....AffirmTrust1)0'..U... AffirmTrust Validation Authority0.."0...*.H.....0.....0B..Ru.EZ.,....o.....p....7.P..H/.h.{?2XK..G7...}w.$..c..=...?..1.....R...[.+.w.h..b+c..x...l./.....'.c..%.....d.z]X..V .g

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2508E8D974CC05F224A38A6A068698E0_79F9901B6CE1C0907957A8D61937ACE1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1535
Entropy (8bit):	7.401483692550266
Encrypted:	false
SSDEEP:	24:9WppAk/bsONwGdp2NfMc2JcziQCBdppAB7McNXppDBuxpD4uE4GrRu4L85+oxwE1:98pAooONv2FMSZCppAxMu5pDBuxeuaYJ
MD5:	5F444521E3FC36067EE484831CDF5938
SHA1:	CAD660FF7698AD935857D4DF2AE76A9E9344035F
SHA-256:	9B4308F89B0136813BAFED5CF43B55AB6723A460EF06F567C7F774A69B801AAE
SHA-512:	AC6E3FFF74EF95C05F37DEBCA476A67B7B0077E12EDDBFA2E8D9FF54B10E0FD3C692459D1538F79D9F0ACD1A7BC91F77E29B63BC35ED64612E209933E9D166C7
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0..P0N1.0...U....CA1.0...U....AffirmTrust1)0'..U... AffirmTrust Validation Authority..20210203085300Z0s0q0l0...+.....m2.Pb....\.t....mW.....e7..G.5.....X1....k!....X.f.....20210203080000Z....20210210080000Z0...*.H.....m..(U.....0..,<.....}p..u....:..3F....".s/....htG.w..0.....AA..n.UP<..yr{sw..}.y.F..=8GM^W34.T..!.....N..=U...c..>..oK'...^b'...OF;....+/.h.Y...$.y..6..D.....}...).....1.[.Ne+.....8q...#9....l...mr@).+.....0.).]K.....W...2..p.\B.;.....$.-.?.....0...0...0.....j.+.....X.cs0...*.H.....0..1.0...U....CA1.0...U....AffirmTrust1+0)..U..."See www.affirmtrust.com/repository110/..U...(AffirmTrust Extended Validation CA - EV10...191101190651Z..221101193651Z0N1.0...U....CA1.0...U....AffirmTrust1)0'..U... AffirmTrust Validation Authority0.."0...*.H.....0.....0B..Ru.EZ.,....o.....p....7.P..H/.h.{?2XK..G7...}w.$..c..=...?..1.....R...[.+.w.h...b+c..x...l./.....'.c..%.....d.z]X..V .g

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\A37B8BA80004D3266CB4D93B2052DC10_994B5C515D64A296EABD42B0A2E46349	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1585
Entropy (8bit):	7.40607371305806
Encrypted:	false
SSDEEP:	24:Bp8UqCEQlBKhB6EWgczgKpffU8hsf52BxUqCEB7/Iajl6E0YprRl3SX+6:Bp8UGQlBGxWgczjU8hscUGx/bPfd6
MD5:	251000A52FAD85BC04B3E760FD0CA9A1
SHA1:	B80F1712A160604F9F78B5960E9C722B85DC768B
SHA-256:	9970CEA9D9BBF518DF3923080749BCE263D9C86384EE63FFAB42FB90DEA3007E
SHA-512:	088B128B931F97014B04F4CC9A3F9986AA60EA550AAAB49E9354FA78DBD1EB650BAEE48E5266CDA21662D410EA31FCE978DA0FB2D43ECD2BBA6C1061BFD49A2D
Malicious:	false
Reputation:	low
Preview:	0..-.....&0.."..+.....0.....0...0..N0L1.0...U....US1.0...U....Entrust, Inc.1%0#..U....Entrust Validation Authority..20210203101800Z0o0m0E0...+.....\...a.....A[B'...jr&z...}.;iQ.l....f...a.....Q.f.....20210203100000Z....20210210100000Z0...*.H.....".:..oF.....c..TY.lK.K.`D.y.ch+...z.X3.....e.+.:..?..gNH....J_Y.[.r!..._uk....a.....-A.k.3y-.S.J...l.rf!.fq......_..Z...1j.....Q.y...M#..<C.4..N....:...l....r.#..;Q...e..D.eF..T..^...X.....j....E/..^..2THY.....SJ. T..x/p.../.....{4..."0...0...0...../.>.....Q.a0...*.H.....0..1.0...U....US1.0...U....Entrust, Inc.1(0&..U....See www.entrust.net/legal-terms1907..U...0(c) 2009 Entrust, Inc. - for authorized use only1200..U...)Entrust Root Certification Authority - G20...201021183945Z..211021190945Z0L1.0...U....US1.0...U....Entrust, Inc.1%0#..U....Entrust Validation Authority0.."0...*.H.....0.....3x.F.'.B..$..-..P@.M....]e..4.B.K..6..p.dk#m'.I.0}X.|...'...8.h..=....;.....<-

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D8A5A4A0441F7653C3609E0E2DE6769F_7CB1F9CF5591E73A1593763D843A4B86	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1585
Entropy (8bit):	7.3916007731098174
Encrypted:	false
SSDEEP:	48:BiUGQ+QjofVU8h23TUGxr5vR0EKJdCgM7sP:aijorGPxtR8DMa
MD5:	3741A41B376A21368760F69CB39793EF
SHA1:	A839DA67D212EA4C35ADA9036EDBD2FA4945EF1E
SHA-256:	B35ACF3C02D3BA119245CAC590CCC8B7A090CE242B6DFFB76FFE7A46882884D4
SHA-512:	08867455D1314DACE38CDAC1812A4AE8EF59D42F0BCB017CBA50F38F7AB33F0BD5072D4B4BE1E73DE84B81808DB0878E813B002DA8AD2D5043723BEF174C007F
Malicious:	false
Reputation:	low
Preview:	0..-.....&0.."..+.....0.....0...0..N0L1.0...U....US1.0...U....Entrust, Inc.1%0#..U....Entrust Validation Authority..20210203173500Z0s0q0I0...+.....'.D.I...X.y...`.....*0....!p9T..p.:..6K.<zp.I.0.~..S....20210203170000Z....20210210170000Z0...*.H.....(.r....:R...0.S.q?.].....@..c....Q)i@7.eEt..4.....%.x.zWM/.xL{>....N.....&.....P..i]`.QBC.!M.Z..&.fv.zQ.]..hE$2M.O^usXAm.M....>.....a|+:.)lwl.'.o...{.....5.'4..K|I..:I.....cN.....qJ...0...5|.....?.&.[.A|...<.7S0.3Vw.....p.PWg#.F].....r....0...0...0.....M...*.....T.x.0...*.H.....0..1.0...U....US1.0...U....Entrust, Inc.1(0&..U....See www.entrust.net/legal-terms1907..U...0(c) 2014 Entrust, Inc. - for authorized use only1.0,..U...%Entrust Certification Authority - L1M0...191101180350Z..221101183350Z0L1.0...U....US1.0...U....Entrust, Inc.1%0#..U....Entrust Validation Authority0.."0...*.H.....0.....fKkj...w)Q;;1_.&-.8...:..m#T...(p:.....t..^O..`.....y..1..+..F...y<.v.xN.P\

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1697
Entropy (8bit):	7.304415166359865
Encrypted:	false
SSDEEP:	48:snitqJzc3HrruVnitqsXA49e5REMeZ6+23wQ:UJowsw49eEMeZ6+Y
MD5:	9E41C5CA971105E16DF1F908DC7815A8

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
SHA1:	75D6A55BCDA138C4F5DF58741015AAB9647B676C
SHA-256:	7CAED1F44B14DC4C9F2EB038CF78EE8386554FBC69D98E3733EC995B864A1A67
SHA-512:	D34865F3ED741499F356E92EEDB87D2BBB01C694E11B05E3749541579D5CEB2FC4335A45004106301A8719E58BD9CF91D257B5CA1AB41F851B3967BB856A418E
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G1..20210202210918Z0f0d0<0...+..... .....]..J^.y_..F<.....L.q.a.=...j.....20210202210918Z....20210204090918Z0...*.H.....eRW.....r.7....f=.....j.....D..1=.....D"....(.+Y.(.,..W.M.)...gP%..x.2.y...pY..f.~...$.1O3..q..b8..S.....8..^-.....U..#.X.....d.g.:S...i.W..AES..)19L....I..ZG.b.....Q.(.,TKV*Af....`..#.=.s.%.....Je.._z...`...4..'..0....b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...161213070000Z..211213070000Z0..1.0..U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G10.."0...*.H.....0.....}...@.H.....j.b.2.c....'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.X

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0C2A6B05AF7011FB1228AE98D31E7D22_906CFB2450238D0B4C3B6D559BA937CB	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	3.8139203915944404
Encrypted:	false
SSDEEP:	24:UVt8snv2rqME7bPUrumaVt8snv2rqME7bPUruD:atmrqMObsr6tmrqMObsrw
MD5:	1F361BB24F4E08CF9676471E35D35FFC
SHA1:	B4314538672075182609641075 3ECD53522A78F3
SHA-256:	664825F05E12963A2B58D2776406E4ADF5A7E3824E282A6F60B8FD8D0EB7B1D3
SHA-512:	FF626F10222B7D360E3689D2B17FB8988B4BA58F5753CEA9DB0434CEF1D70478588658807C3EFB38A3B9A495B5545573894BFC5D3636B3610B7CDE3F29DE6ACE
Malicious:	false
Reputation:	low
Preview:	p..... ....(..... .....h.t.t.p.:././.o.c.s.p...a.f.f.i.r.m.t.r.u.s.t...c.o.m./.M.E.k.w.R.z.B.F.M.E.M.w.Q.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.0.%.2.B.T.g.T.F.B.d.h.t.T.l.P.i.t.m.k.9.u.x.W.I.9.j.H.d.Q.Q.U.n.Z.P.G.U.4.t.e.y.q.8.%.2.F.n.x.4.P.5.Z.m.V.v.C.T.2.I.I.8.C.C.E.D.w.u.6.q.K.4.M.C.Y...".F.D.B.3.2.A.8.6.5.2.2.D.1.F.2.E.3.F.F.6.2.9.5.F.F.1.A.0.0.E.F.0.8.8.D.4.F.6.F.3.A.1.6.8.2.0.1.9.3.4.9.F.1.1.5.C.8.4.C.6.9.7.1.B."...p..... ....(.....(.....(.....(.....h.t.t.p.:././.o.c.s.p...a.f.f.i.r.m.t.r.u.s.t...c.o.m./.M.E.k.w.R.z.B.F.M.E.M.w.Q.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.0.%.2.B.T.g.T.F.B.d.h.t.T.l.P.i.t.m.k.9.u.x.W.I.9.j.H.d.Q.Q.U.n.Z.P.G.U.4.t.e.y.q.8.%.2.F.n.x.4.P.5.Z.m.V.v.C.T.2.I.I.8.C.C.E.D.w.u.6.q.K.4.M.C.Y...".F.D.B.3.2.A.8.6.5.2.2.D.1.F.2.E.3.F.F.6.2.9.5.F.F.1.A.0.0.E.F.0.8.8.D.4.F.6.F.3.A.1.6.8.2.0.1.9.3.4.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	900
Entropy (8bit):	3.7348418988130954
Encrypted:	false
SSDEEP:	12:meDOsrQESIgsFFV13Mz1mySGqQj3Xe8/srQESIgsFFV13Mz1mySGqQj3a:hwyPV13MhmyFq0UwyPV13MhmyFq0a
MD5:	F3C01CB930DDD28E7253BBEE918C3FA3
SHA1:	3D33B5AFA18B52A722CDA5F1C9DB3B7BD4ACA576
SHA-256:	7B27B5886D3C3FC901FB3D8051A280A4F099E4E130EFEF5C7581974BAA42C7B6
SHA-512:	B3CB971733DE4D5CDF659AA79F080600C6FEC5BCF036A23428023A142D32FAF0981040C3693443CC416226F13FD997ECDA944DE331DCF00AF2FA72B80BDCF2
Malicious:	false
Reputation:	low
Preview:	p..... .....G-=....(..... .....@d.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m./.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.l.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".b.6.4.6.7.9.1.1.4.7.c.7.3.a.7.7.b.6.1.e.3.5.0.e.9.3.2.f.f.8.3.0.6.4.0.c.f.4.c.a."...p..... .....G-=....(.....@d.....O.....O.... .....@d.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m./.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.l.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".b.6.4.6.7.9.1.1.4.7.c.7.3.a.7.7.b.6.1.e.3.5.0.e.9.3.2.f.f.8.3.0.6.4.0.c.f.4.c.a."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2508E8D974CC05F224A38A6A068698E0_1FA4F51F50E531077AD3338680850105	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	3.7955515523871663
Encrypted:	false
SSDEEP:	24:0+8xv5EtXrbiyI320Si778xv5EtXrbiyI320Sim:0+kEtniyi2Zi77kEtniyi2Zim
MD5:	7EC18E640026AFE90EC2027FBCC346E8
SHA1:	ED7B3610CD6B9FC0BBCA3FCB607C4ECF79BBA6BA
SHA-256:	28954C25315C46721EE734D3951ECD1DB3A9E34D06A341731990BADE0A8CAEE8

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2508E8D974CC05F224A38A6A068698E0_1FA4F51F50E531077AD3338680850105	
SHA-512:	048E17FB03C74B67E5F81655870404D39428C277B7BBC0D64A94569229A64F84A72785369A811137678DECD4830063C7A82DB88715178C99C065CFE573E88D61
Malicious:	false
Reputation:	low
Preview:	p..... ...."..........(..... .....h.t.t.p.:././.o.c.s.p...a.f.f.i.r.m.t.r.u.s.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.t.M.h.Z.Q.Y.p.q.o.2.x.x.c.F.X.S.x.t.J.G.r.b.V.c.L.y.g.Q.U.2.%.2.B.9.l.N.w.v.l.R.8.s.1.0.Z.A.f.A.8.G.8.i.M.e.n.6.o.A.C.E.D.r.Q.B.s.Z.r.S.A.y.J.A.A.A.A.A.F.g.I.S.P.E.%.3.D...".A.7.4.0.9.B.7.4.F.A.E.2.E.7.2.6.0.6.9.1.5.2.3.F.1.D.9.8.E.9.6.6.A.8.1.0.B.B.5.2.D.B.A.8.3.5.B.4.4.1.3.9.9.4.F.7.6.E.A.2.3.2.F.0."...p..... ...."..........(..... .....h.t.t.p.:././.o.c.s.p...a.f.f.i.r.m.t.r.u.s.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.t.M.h.Z.Q.Y.p.q.o.2.x.x.c.F.X.S.x.t.J.G.r.b.V.c.L.y.g.Q.U.2.%.2.B.9.l.N.w.v.l.R.8.s.1.0.Z.A.f.A.8.G.8.i.M.e.n.6.o.A.C.E.D.r.Q.B.s.Z.r.S.A.y.J.A.A.A.A.A.F.g.I.S.P.E.%.3.D...".A.7.4.0.9.B.7.4.F.A.E.2.E.7.2.6.0.6.9.1.5.2.3.F.1.D.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2508E8D974CC05F224A38A6A068698E0_79F9901B6CE1C0907957A8D61937ACE1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	3.778585071286952
Encrypted:	false
SSDEEP:	24:ng/98xv5EtXrbiyIC5oxTH76898xv5EtXrbiyIC5oxTHL:ng/9kEtniyUTH7689kEtniyUTHL
MD5:	E889EAFF9C731F488367EE7934F44276
SHA1:	9EB5AAC31BE1383997FC8BD58B0BFDB7EDBA84F7
SHA-256:	AD9055650591D538544B23CE88E276D381C44C2C56E55E8DF16E3A7F65DAA1F6
SHA-512:	F37D22A15C917E8BA335CAA3EDFBFC1F315F14DA7B60FC722CDC14728CBBE2A6D963A8515A3D1399DCBCCE11A68B72C3EC70DB5AFB2E6E62D303CA01448DD422
Malicious:	false
Reputation:	low
Preview:	p..... ....&..."Jxe....(..... .....W.....h.t.t.p.:././.o.c.s.p...a.f.f.i.r.m.t.r.u.s.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.t.M.h.Z.Q.Y.p.q.o.2.x.x.c.F.X.S.x.t.J.G.r.b.V.c.L.y.g.Q.U.2.%.2.B.9.l.N.w.v.l.R.8.s.1.0.Z.A.f.A.8.G.8.i.M.e.n.6.o.A.C.E.F.g.x.%.2.B.K.6.U.r.W.s.h.A.A.A.A.A.F.g.I.Z.h.g.%.3.D...".9.B.4.3.0.8.F.8.9.B.0.1.3.6.8.1.3.B.A.F.E.D.5.C.F.4.3.B.5.5.A.B.6.7.2.3.A.4.6.0.E.F.0.6.F.5.6.7.C.7.F.7.7.4.A.6.9.B.8.0.1.A.A.E."...p..... ....&..."Jxe....(..... .....W.....h.t.t.p.:././.o.c.s.p...a.f.f.i.r.m.t.r.u.s.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.R.t.M.h.Z.Q.Y.p.q.o.2.x.x.c.F.X.S.x.t.J.G.r.b.V.c.L.y.g.Q.U.2.%.2.B.9.l.N.w.v.l.R.8.s.1.0.Z.A.f.A.8.G.8.i.M.e.n.6.o.A.C.E.F.g.x.%.2.B.K.6.U.r.W.s.h.A.A.A.A.A.F.g.I.Z.h.g.%.3.D...".9.B.4.3.0.8.F.8.9.B.0.1.3.6.8.1.3.B.A.F.E.D.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.090852246460565
Encrypted:	false
SSDEEP:	6:kKtihkpbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:EOw3kPlE99SNxAhUeo+aKt
MD5:	29DCABE51D8A8E7BAE76EE2960EC7E55
SHA1:	80FAE178EF40300C41A7D3E7CE3FE85375606E5B
SHA-256:	BD97FE56C3506AD65B1FB5A6E8D60B4994C95DDF477419FD2B648F33240EC8D1
SHA-512:	0AE44572D27591A82B5388DDD5EFA48822F77C3D597BD2B69A008092B2F1CFD62AAF8DB6A2130357D71C7D724D7C92746CB2D3F0E02C2580F405DD4CA4A952
Malicious:	false
Reputation:	low
Preview:	p..... .....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A37B8BA80004D3266CB4D93B2052DC10_994B5C515D64A296EABD42B0A2E46349	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1048
Entropy (8bit):	3.759275456076191
Encrypted:	false
SSDEEP:	24:OH9LmvNrg5ubxwfC0nbH9LmvNrg5ubxwfC0d:OBaIubxwK8bBaIubxwKK
MD5:	AA0925F377C3CE29E05FD6BF9A640309
SHA1:	45DF9D66259A56D9E6BAE0F93354D511CD0119DE
SHA-256:	3B36E72DD433A99472D7902139B3695C9010B4DC6EF2FE37E71E931D78D79518
SHA-512:	D1AC3700137E71E014427315B2D11C51F17A0A30046BE900FD1B06FB57C713D762D4F52F945B9598A5C872BFA852DF3B6163C755104FD1D032B9BE2D34776041
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A37B8BA80004D3266CB4D93B2052DC10_994B5C515D64A296EABD42B0A2E46349	
Preview:	p..... ....B.....(..... ........P.U....f.....1...h.t.t.p.:././.o.c.s.p...e.n.t.r.u.s.t...n.e.t./.M.E.0.w.S.z.B.J.M.E.c.w.R.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.L.X.N.C.z.D.v.B.h.H.e.c.W.j.g.7.0.i.J.h.B.W.0.I.n.y.w.Q.U.a.n.I.m.e.t.A.e.7.3.3.n.O.2.I.R.1.G.y.N.n.5.A.S.Z.q.s.C.D.G.G.h.5.9.I.A.A.A.A.A.U.d.N.m.p.g.%.3.D.%.3.D...".9.9.7.0.C.E.A.9.D.9.B.B.F.5.1.8.D.F.3.9.2.3.0.8.0.7.4.9.B.C.E.2.6.3.D.9.C.8.6.3.8.4.E.E.6.3.F.F.A.B.4.2.F.B.9.0.D.E.A.3.0.0.7.E."...p..... ....B.....(..... .....P.U.....g~.....g~.... ........P.U....f.....1...h.t.t.p.:././.o.c.s.p...e.n.t.r.u.s.t...n.e.t./.M.E.0.w.S.z.B.J.M.E.c.w.R.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.L.X.N.C.z.D.v.B.h.H.e.c.W.j.g.7.0.i.J.h.B.W.0.I.n.y.w.Q.U.a.n.I.m.e.t.A.e.7.3.3.n.O.2.I.R.1.G.y.N.n.5.A.S.Z.q.s.C.D.G.G.h.5.9.I.A.A.A.A.A.U.d.N.m.p.g.%.3.D.%.3.D...".9.9.7.0.C.E.A.9.D.9.B.B.F.5.1.8.D.F.3.9.2.3.0.8.0.7.4.9.B.C.E.2.6.3.D.9.C.8.6.3.8.4.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D8A5A4A0441F7653C3609E0E2DE6769F_7CB1F9CF5591E73A1593763D843A4B86	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1096
Entropy (8bit):	3.808341744430903
Encrypted:	false
SSDEEP:	24:xOHYvPig2i7B3dK00jS7TEOHYvPig2i7B3dK00jSX:xOa92iF3NwS7AOa92iF3NwSX
MD5:	AA9AB5B0CC4DE8E8681D1483685758C4
SHA1:	C0EAD5D000A82EA8F00BCC5864476CBABEB5AD60
SHA-256:	4E1DE4544546BE923FE167515042738483B7070F289DBA15A2C79709DC693595
SHA-512:	57CB7A6A4BFB400B5C4A3D0828A65A7B3AB9EC83A3D326090E416FF4C24F41057D9416B6DD3F5DEE380D5E397D1DE2301E606B1470E12C2FD442BF1C6EF3160
Malicious:	false
Reputation:	low
Preview:	p..... ....*.....$....(..... ....(..N.....1...h.t.t.p.:././.o.c.s.p...e.n.t.r.u.s.t...n.e.t./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.n.u.E.Q.c.S.c.L.%.2.F.k.l.j.K.e.d.%.2.B.R.z.p.z.F.Y.O.q.9.k.w.Q.U.w.%.2.F.f.Q.t.S.o.w.r.a.8.N.k.S.F.w.O.V.T.d.v.I.l.w.x.z.o.C.E.D.Z.L.y.z.x.6.c.L.V.J.u.j.C.L.f.s.G.%.2.F.U.%.2.B.E.%.3.D...".B.3.5.A.C.F.3.C.0.2.D.3.B.A.1.1.9.2.4.5.C.A.C.5.9.0.C.C.C.8.B.7.A.0.9.0.C.E.2.4.2.B.6.D.F.F.B.7.6.F.F.E.7.A.4.6.8.8.2.8.8.4.D.4."...p..... ....*.....$....(.....(..N....h.*.....h.*.... ....(..N.....1...h.t.t.p.:././.o.c.s.p...e.n.t.r.u.s.t...n.e.t./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.n.u.E.Q.c.S.c.L.%.2.F.k.l.j.K.e.d.%.2.B.R.z.p.z.F.Y.O.q.9.k.w.Q.U.w.%.2.F.f.Q.t.S.o.w.r.a.8.N.k.S.F.w.O.V.T.d.v.I.l.w.x.z.o.C.E.D.Z.L.y.z.x.6.c.L.V.J.u.j.C.L.f.s.G.%.2.F.U.%.2.B.E.%.3.D...".B.3.5.A.C.F.3.C.0.2.D.3.B.A.1.1.9.2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	916
Entropy (8bit):	3.7670887766876273
Encrypted:	false
SSDEEP:	24:7KzV4xaVSGAmqBBRMf8dTzV4xaVSGAmqBBRW:7mVnMGBS6iXVnMGBSM
MD5:	089B32548E4D0F1A0389D3EDEF180E5F
SHA1:	4352150E6E292326882C0B46E94C394E13754306
SHA-256:	A4CD1C33730B7E9E3C7EA6CC413B17D2C6889A8A92779BE19C6C1A9DF072F042
SHA-512:	B940EDBF04D8BC58887CB9F260FAF2A9E286ED93AA87C7490F29C032C73CCF76BAD7133FFC2103A82C424FA69871021848BDD433498E15511D84DC09C3D937E
Malicious:	false
Reputation:	low
Preview:	p..... .....[.<....(..... ...."........V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.I.3.I.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".7.5.d.6.a.5.5.b.c.d.a.1.3.8.c.4.f.5.d.f.5.8.7.4.1.0.1.5.a.a.b.9.6.4.7.b.6.7.6.c."...p..... .....[.<....(....."....."....j.....j.... ....."....."....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.I.3.I.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".7.5.d.6.a.5.5.b.c.d.a.1.3.8.c.4.f.5.d.f.5.8.7.4.1.0.1.5.a.a.b.9.6.4.7.b.6.7.6.c."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\05fe5c1e-4746-4d06-a5e4-b8f54d0d89ef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	357884
Entropy (8bit):	6.02869206809332
Encrypted:	false
SSDEEP:	6144:lkz9nifaEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinz:enCGNPUZ+w7wJHyEtAWi
MD5:	23F5B75773C0737B31F897E90677E961
SHA1:	B338DB0821072F24B061062705E96EA6EB1C1ECD
SHA-256:	783404489A5265AE966C50F637845454996C2B5E261935B49399BC7AB41CB9AA
SHA-512:	AEE3594A31CCCB6D2CB3F08DCBEF0F5D24D505107849002841C9763A265EEBCD8B4B0E7F83F2D6325970D4A7E7E3F5785BB302D839C2B3AC69B3FC43C28FE3C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\05fe5c1e-4746-4d06-a5e4-b8f54d0d89ef.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612410601219635e+12,"network":1.612378204e+12,"ticks":155175585.0,"uncertainty":4467198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488234204"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\06f4c19f-9055-4202-a3ed-61cce8892560.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	366356
Entropy (8bit):	6.050314082741428
Encrypted:	false
SSDEEP:	6144:3kz9nifaEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinz:UnCGNPUZ+w7wJHyEtAWi
MD5:	2066A06FE2FFA7C83EA724653CA0F19E
SHA1:	E535FF911C46E6ED9F1D93D550D4C1E1812BE174
SHA-256:	2CB036C2BA518C706D8115C67A1C296DEB7453158BF0B54F3CE8F216070F8F50
SHA-512:	D93D4E373AFBED112E0D86A6AA9B8135498E60002707677BB4DF6E3735427F7A1430BBE7F904E50DD188B1D64443EA558F4743F4EB26C964D8F146F0251B7991
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612410601219635e+12,"network":1.612378204e+12,"ticks":155175585.0,"uncertainty":4467198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\12ad13b7-4ddf-4e8b-b350-14d42be72735.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7451329433296308
Encrypted:	false
SSDEEP:	384:h/l66EXFYP42VvB+xNSrHvGu39WIFHwdGpQr7o2Mx1Y8oPrnemrILYSS+xOY0yN/:xm+RZqgpRQeXAicY3f22KQ+C5b
MD5:	C912575A9D42BD49CDCDB38D25F6C509
SHA1:	437FC3766E5E13395EF8F3C895E9EC9945BB69C6
SHA-256:	F53AAF4711C3808B0D7C163A3DE10EFDE2EE763CD92791BE2159E39C1D2B5AD5
SHA-512:	F7D44D4BF4A953BCCB3EFFCCDD0B36425FDD9C85F927B69F36E9BAA51CC9700C8133AD47ECA9B69A8E3BFA2F58C2E0853C1B42AF7E61BD4FA9F17B96F04C8A65
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....08.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\3ab3e183-b81a-41d3-8ff8-fe5f966f25bf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	366356
Entropy (8bit):	6.050314215355406
Encrypted:	false
SSDEEP:	6144:Xkz9nifaEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinz:0nCGNPUZ+w7wJHyEtAWi
MD5:	14D9D4F8441556B8F500928B308B776D
SHA1:	E99BFC1159FF4637E0C23250FB30F314988CB078
SHA-256:	0553D43C64E05A70E94F0A8CFDF16C1AE151F4F615FFC118BBA6393243AE4C0A
SHA-512:	B32A89C332B576324025C337B78F670212332BA095A2FFF9B31660772B0130D6EC74C08F216A45D801A2725A8DAD75B5A1AEA8A89BAA8E925D8C737EE0BAD7FE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\3ab3e183-b81a-41d3-8ff8-fe5f966f25bf.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612410601219635e+12,"network":1.612378204e+12,"ticks":155175585.0,"uncertainty":4467198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488234204"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4cfea814-af7f-4e81-a970-3e1bc892084e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	357884
Entropy (8bit):	6.028691990463783
Encrypted:	false
SSDEEP:	6144:Lkz9nifaEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinz:wnCGNPUZ+w7wJHyEtAWi
MD5:	203AFD1872A709A309A3D332B5ADED31
SHA1:	1EAE7D9EE85FE9A6504B8D5A14A6C1DF38D7A0B5
SHA-256:	6BBE30A51E085DFCEB9FF61816334731C8C1F5A48CB65305E3DD38E5BA2F28B1
SHA-512:	A2C6594237551EE18941EA1786A2ED9BB288FA8CB7A066786735CEA5868BF1C234C4D9FF33C2E496F9FD385BEE3AD80316C37B8A625CCEE6EB0398750A56420
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612410601219635e+12,"network":1.612378204e+12,"ticks":155175585.0,"uncertainty":4467198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488234204"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6b39e29f-1a02-4a57-834a-6fa84c208bc6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	366355
Entropy (8bit):	6.050314284724828
Encrypted:	false
SSDEEP:	6144:9kz9nifaEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinz:mnCGNPUZ+w7wJHyEtAWi
MD5:	A791160722BB8EF7F83710CA63504131
SHA1:	8EE915FF94ED51E19D73C8184498F3D8A0C076D3
SHA-256:	C2A53CF09A80482232F8D469F4DE63418B604C25A373875A3AC547063B7550E2
SHA-512:	40397DA7D357CA338597F284BB07CBA6F849B78D875BB620DCA71E50BF7F17E60F185107019CF5B2F7AF4891545269A79B2C44AE0982DD3C0AD463AAC0E3FE2
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612410601219635e+12,"network":1.612378204e+12,"ticks":155175585.0,"uncertainty":4467198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f4cdda7-cd17-4037-9caf-53381fdac500.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	366355
Entropy (8bit):	6.05031420509673
Encrypted:	false
SSDEEP:	6144:pkz9nifaEG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinz:qnCGNPUZ+w7wJHyEtAWi
MD5:	48E5AF046BFE49CA685AB01A03AE41F5
SHA1:	4E3CAE8F2EB37B29CCEE91C76E61A996ABFBD3E1
SHA-256:	6FFE1986567757BF28A3A570B19505E42BB54642C852D64A6222718980AC3FE9
SHA-512:	960DFC59ED59C71307D46BD0004CE2E99B55B47AD1E0F7FA4D5BC46337E6ECF87B988E4C3EFE4BDEFFF8D26980F447B6135E61689EFC241E505F32E4C5CA26C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f4cdda7-cd17-4037-9caf-53381fdac500.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.612410601219635e+12,"network":1.612378204e+12,"ticks":155175585.0,"uncertainty":4467198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\072b894c-01b5-4e89-9844-7609209a8413.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1096b430-6533-413c-a6fe-700abe74f8cc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3043
Entropy (8bit):	5.583085162087315
Encrypted:	false
SSDEEP:	48:Y3UIOeUd5UEieUjEUN6UUhcND+Ux7ULUBUsUADKUA2BsmU5bX5U83UbaUeVNwUOw:yUIOeUfUEieUgUkUUaND+Ux7ULUBUsU3
MD5:	ED9451207A0BB393C2414D2739930CA2
SHA1:	4CF06BDDE10A31CEA0F645EB7333CD9D6371463A
SHA-256:	DCE5F12E4BDFD08C2264C79ACD3CFAA56BE591EC95AD52345EF6AA9A8F9AB313
SHA-512:	DA964A269E24F99EB3CE8BFC38130FF74B86D4AF30D5207F24B3A2B3B80441032AA003072B77CE56D6D24FE4CB2BBE3E080233366962EB5DD12D7388A50B67D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1615002844.391176,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410844.391183},{"expiry":1623297244.67959,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410844.679596},{"expiry":1643946848.653427,"host":"MztrKzIr9UYddfdUE9hZboO5anJ2Et4vIn4Q67H/i6E=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410848.653433},{"expiry":1643946714.457025,"host":"M4bfUnCmQAi4PNb3B8al/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410714.45703},{"expiry":1643946720.817906,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410720.817912},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\14c2d5b3-d481-4abe-8b7e-0e9a5b403260.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16763
Entropy (8bit):	5.578315235392654
Encrypted:	false
SSDEEP:	384:+h5tqLlGRXa1kXqKf/pUZNCgVLH2HfDOrUBSNW42:9Llma1kXqKf/pUZNCgVLH2HfSrUBoWB
MD5:	BDBF6FABCAC1BA960FA0F694428693D8
SHA1:	B01AB38B4A3366FA11733C0A37952AB2A30732B3
SHA-256:	77A206D44F5B67EE36B54C60D074CC3B6B67B4946429427EE428A726B51F6FFD
SHA-512:	5A829D5262A3F298D8F01123A8CA6714133F6AACA412891D26750361F006FB75B32832F8BBE0A56CA221E787A484B0D597BE397FAE2EA65A412950B3AF141E84
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13256884198201421","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\21730865-840d-4481-958f-26dda0af949e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22613
Entropy (8bit):	5.535715742911906
Encrypted:	false
SSDEEP:	384:+h5tbLlGRXa1kXqKf/pUZNCgVLH2HfDOrUTHGlnTJBUW4Le:yLlma1kXqKf/pUZNCgVLH2HfSrUzGlnx
MD5:	56AA08564412C025330DF5BD4F671E7D
SHA1:	E8D0936F889D8FAC023E463973A8E17CD1B5F7CD
SHA-256:	CB1202F3FEA96A8B92C262C7FA0B28A3558ABD9602C9FDBDCE6277A303218772
SHA-512:	84195B7273349C69787BD746D1F38CB77CB9C45F621EFDFB734498752BB18651C7B44D798392D5292F0C7888E3DF37D0433B0E339796F67BD69E3512C4E47B67
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13256884198201421","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7437324c-1854-4ffc-b2b4-7ecc65c8738d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5081
Entropy (8bit):	4.971442955501115
Encrypted:	false
SSDEEP:	96:nRVoFGqm4paAVnRxk0JCKL8EkRp1f6jbOTQVuwn:nRVorm4p9VT4Knk7BU
MD5:	04067CA6D2DE5886C4FF3A640F1D46FD
SHA1:	505C14F2C9E56DB5B129BA9E4773E09C869BB051
SHA-256:	34EF9FA854A531EE9DC9ED52631F427BCABBD6C10273009FD9C2B64BD1C59939
SHA-512:	28BDEE6055F563A0AA2C01FA3A8733FC139959B934CF4D1BA754BD0EFB687D6BBDA23205B7E7B8B9BF4EFB4F3E84B8DB3BAB1284C7439FB55BD8E8E59E4093CB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13256884198430602","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b24153b-3089-4657-bc7f-1196e24e6b45.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7b24153b-3089-4657-bc7f-1196e24e6b45.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3210
Entropy (8bit):	5.577964096095608
Encrypted:	false
SSDEEP:	96:vGUKoeU3U5ieU1UCUUaSD+U7UfgNU/UBUsU2KUA2FUeyUUN3U9aUZUEUD:vGUKoeU3UHU1UCUUaSD+U7UYNU/UBUsm
MD5:	C96FDD72ED9390A12FC223A88D4DF316
SHA1:	E72A01EB61A503B379FF75DDC3C28E4846A79350
SHA-256:	0A0E47390A3B1D0476FDEFB9D5EA098E5DA70D6EE23C9457A1CCB11FC5B6C530
SHA-512:	E0C626054B0F0337D109805B22FFB9ADBA9B2B86520FE044B1DC7B69B9F4A3A335299C86FE7BC7C937F60C48E6B5073F3BB12D6F019C6A69FE1AB990395F573A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1615002891.522794,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410891.522799},{"expiry":1623297291.583669,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410891.583674},{"expiry":1643946892.500453,"host":"MztrKzIr9UYddfdUE9hZboO5anJ2Et4vIn4Q67H/i6E=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410892.500461},{"expiry":1643946854.935221,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410854.935228},{"expiry":1643946860.902124,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1612410860.90213},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\81a09fc3-901b-48b2-a1ea-8506c2f16f0c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22614
Entropy (8bit):	5.535641523022977
Encrypted:	false
SSDEEP:	384:+h5tbLlGRXa1kXqKf/pUZNCgVLH2HfDOrUTHGunTJBtW4s:yLlma1kXqKf/pUZNCgVLH2HfSrUzGunM
MD5:	F20FCF21019E6EE4FA247E26FE05D3E7
SHA1:	E417A06FF47A73050BEA667B44F9ED6C02A204E3
SHA-256:	7501F5BDCDED03BF275B081092203666A58862D7976294345422A5F66747A47D
SHA-512:	2CA00C96952C3015A196A9AC9E31F8CB1DA59C46120431D323B3A52E6D7F655B11EEF0E0E14D3C3B5C82248F820413C0B91910934B7C55FD1057511185F9E884
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13256884198201421","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8a345bb5-7d51-419f-b6fe-6a34e791b7cf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	4404
Entropy (8bit):	4.8674501528942065
Encrypted:	false
SSDEEP:	96:2lNnOTXDHzGAelMa3xCJKGLJN8tAGEQG5VVGs5GnnzlxtGnhS:2lNnOTXDHzGAelMa3xCJKGLJ+tAGuVVj
MD5:	7534723A6A8C1D5F57E29D9124A6F8CA
SHA1:	A490E358B071A88D40404DB8A4353F71C4C385BE
SHA-256:	39A979C685E054FF6AAAF451E23C25E720526250BC7187459EB0B8998721ECE6
SHA-512:	3E014414A5307DFB6E10572668AC6598ED44595886E127546888D43D85A77D3119EB9B296680F39CA23BBF5086FD0C46D4F7F934B9716D722B87C2EF1911E567
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13259476201198244","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13259476201200053","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Size (bytes):	340
Entropy (8bit):	5.120316149397501
Encrypted:	false
SSDEEP:	6:m4fHHUkq2PN723iKKdK9RXXTZIFUtpRfRZmwPRf+kwON723iKKdK9RXX5LJ:JH0kvVa5Kk7XT2FUtp5R/P5+5Oa5Kk73
MD5:	29CCC4D34F7BD41807258FEE44CFC1C1
SHA1:	8C660758932EEF0110C7A63301AC09B7EB8F2ED7
SHA-256:	71F237A12BC75B6846B16149C942780F2DA40BD47D7C1A6D87839C787E108A02
SHA-512:	96E233346445375EF036839F97A01912BE0D9DDD2D773379D7B1443654C8CE8C58E818DB81AEE6BD3A2A26453468565F71801169D6C6B2B27B7FA831AD5FE4EE
Malicious:	false
Reputation:	low
Preview:	2021/02/03-19:50:10.308 18d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/03-19:50:10.310 18d0 Recovering log #3.2021/02/03-19:50:10.311 18d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.11515263122123
Encrypted:	false
SSDEEP:	6:m4fMfGOq2PN723iKKdKyDZIFUtpRfMTXZmwPRfMfEkwON723iKKdKyJLJ:JMLvVa5Kk02FUtp5MTX/P5Mc5Oa5KkWJ
MD5:	8D665F04767A1CEBE3F2B2A8934E184B
SHA1:	D35C78983F4FB62C43D5E67667C013E20E7C1F00
SHA-256:	1E463AB1603227CDC3A933A5F019DD491A601D13CBF241BC60021D77DFE1BC51
SHA-512:	4E7562FAFECB2C21BAF5AF2D785F33DFEA461094EC480413AFACD0001B552DF7C9DA3521C88CB8B360401CF0DCAF4790C8FE1469203F51DA60D89411B89C704
Malicious:	false
Reputation:	low
Preview:	2021/02/03-19:50:10.288 18d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/03-19:50:10.290 18d0 Recovering log #3.2021/02/03-19:50:10.291 18d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00a1982a45dd042c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42750
Entropy (8bit):	5.775234691557821
Encrypted:	false
SSDEEP:	768:4I4hevZels90TV8fKS8n9iX7DW0CUCIR9G:oeci+TV8W0RCf
MD5:	FDC13007F248818F8FFDCE6748471738
SHA1:	2D688661CB57A942A5CC4D11454E7123CCC06D6E
SHA-256:	7603C20BB29F93C057A6D63C6DCA9ED3AA6BF788F5C279845E113C0B05ABF8B0
SHA-512:	193AD8086823D2DA53DFB3A0DB4F9B798D5ED301418BE8B8F8AC660B58A4AB073ABC4873B837EA22BEF7AAEB2FABD46FAFCF35337A4D614FA0EF665AE92C9438
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....oh...._keyhttps://js.driftt.com/core/assets/js/38.feef3c6b.chunk.js .https://driftt.com/1uC.../.....vm[..{.z....._6=\zm...K...A..Eo.....A..Eo.....1uC.../.....vm[..{.z....._6=\zm...K...A..Eo.....n."....'.\....O.....h.....|.....4.....(S.l..`....$L`.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push....`.....L`.....`.....Ma....L...`.....a.....Qb..|t....jrvEC.(S....`.....].L`.....i.Rc0.....QbFd.....r.....M....S...Qc...O....__values..Qc.....__read....Qc".1.....__spread..Qbv.....s.....Qb..F7....c.....R....Qb.,(.....l.....QbzG|.....p.....Qbv.47....d.....Qb..D(....h.....QbRF .....f.....QbN.h,....v.... Qf.....tslib_es6_extends.....QbF..)...._.....Qe.U;.....tslib_es6_values..Qej.!.....tslib_es6_read....Qe:.3`....tslib_es6_spread..Qb.f.....y.....Qbv].....m.....O.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\01c430a9b102894d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	86274
Entropy (8bit):	6.008197064837332
Encrypted:	false
SSDEEP:	768:b5Tl1tdGoxTqaHEaPdAszO8tiXKEOR0nj5Tl1tdGoxTqaHEaPdAszO8tiXKEOR0C:n3dGOmaomazP3dGOmaomazC
MD5:	79F14DD66089C990DF2CCD4DC345E24F
SHA1:	9769C73E90C25B88DCCA7659199A0E5C23F27FFB
SHA-256:	0B28012572BB4D041F4621947B06BB44C4FD5A55F6DB3436EF1699443178277E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\01c430a9b102894d_0	
SHA-512:	17BBE0498B57CECE0A115A926D4E44AEDADC9E5F2F79161C2E0E8E19C19BA31CE84FB3EC50E9F55C468D2EE9676D80C0A0A0022005A3629557AAFEAD6B1F0 F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...0r<...._keyhttps://js.driftt.com/core/assets/js/26.91e0f92d.chunk.js .https://driftt.com/pDP.../.....V..h.o*S....jt.....A..Eo.....6.....A..Eo..... .....pDP.../.....V..h.o*S....jt.....A..Eo.....#[.....'..k....O.... ....N.....(S....`n.....L`F.....Qc.....window. ...Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....4...`.....a>.....Qb6!.V....0O9JC..Qb.....ERkPC..Qb..<.....IR/NC..Qb"..(....Lf9qC..QbV.....QS5 2C..Qbnz.Q....UAFNC..Qb.....ZO/3C..Qb.O3O....c58oC..Qb.....h7FZC..Qb~.....hLw4C..Qbfi.....hf2PC..Qb..d.....jiMjC..Qb.V|.....l9C+C..Qb...x....lEaqC..QbnJ-Q....qn4 dC.(S....`.....L`J....hRc0.....QbFd.....r.....R....Qb..F7....c.....QbzG|.....p.....QbRF .....f....(Qh..."...._possibleConstructorReturn....Qb.f.....y....4Qk.d5C'...BrowserRoute r_possibl

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\03ca1713717c7b03_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38106
Entropy (8bit):	6.099291953230721
Encrypted:	false
SSDEEP:	768:X0Joh74QsmRwJ3uEmlwZSrdBMUZnUimZ34z:X0AdsmCdjAc6oU434z
MD5:	8D9D804B39D39363EB7C6360C8AFF4BB
SHA1:	9471814BB70878DCAD1EE64F14AC45559DB38F95
SHA-256:	8033B25D2AB52EFA101C1CAAA143A7D2E9A6BF5EC0DEEA876EDE5BB9C1E30D2A
SHA-512:	FDEB41BDC79396C6510885C0E459830699078DE3688467408CF2B1966EBC3D54767E59734280BA1FC10D64888404A7CD4C307A714778D779F0CACC89A8780545
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....it...._keyhttps://js.driftt.com/core/assets/js/14.274c57c3.chunk.js .https://driftt.com/..V.../.....}.n.....TU.~H..&.b.....D..A..Eo.....A..Eo..... .....'.L.....O....8...P-.w.....0.....`.....(S.....`.....L`b.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.. .....`.....Ma.....`.....aZ.....Qb.....12GJC..Qbn. m....2VrWC..Qb.....8eKLC..QbZ..p....BZgGC..QbZ.....CwrGC..Qb.ji.....P6DiC..Qb.o8.....Q0X4C..Qb..M.....Q80 rC..Qb.t$^....Qp3aC..Qb*..J....RJSHC..Qb.cY.....UwV1C..Qb...:....WkzbC..Qb6..H....ZGTzC..QbB.N?....ZP32C..Qb...S....fmuzC..Qb.....mQ2CC..Qb2.d'....n/d+C..QbJ L.....noexC..Qbje.....oImbC..QbF#.....p0+KC..Qb..: ....sZBtC..Qb.S0.....t/7OC.(S....`.....`L`,.....RcX.....$.....S...QbFd.....r.....Qb..F7....c.....Qb.`.....o.....Qbv.....s.....Qb., (.....l.....Qbv].....m.....R....Qbv.47....d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\03cf3aa0642e3d9a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.863375070678543
Encrypted:	false
SSDEEP:	12:iVx4Ie0VZSIHnphSNTF/mIHnphyLCwFR8nph:iVWgZnXuTFbXyewFR8X
MD5:	6D829E97735C7F4D963C24FD32FC3431
SHA1:	FCA1E1DF30522F965BE9202054A987972B30B61A
SHA-256:	177394B32E83607855E6F28F203EF955A405DA409B808BF61C2272ECB9C37C4F
SHA-512:	E1A8DCEF2630BC19D6C19301969ABC26BE2C99506491F53ED1BBBEF901AFDC363AC404A5405619BF50B337DBFCE59F91248F1EBE12E14044AA75B11C62B090 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...phXC...._keyhttps://js.driftt.com/core/assets/js/29.69384517.chunk.js .https://driftt.com/^wC.../.....(.....n.C.....V.....A..Eo.....'.....A..Eo..... .....^wC.../.....(.....n.C.....V.....A..Eo.....)..4.....^wC.../.....26106C09CFA41A7052C57DD4620BEE069F46C5132AABF9CA4B1DE4AAD3397753. (.....n.C.....V.....A..Eo.....;L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05fcd8b85e1b3284_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.480976546993909
Encrypted:	false
SSDEEP:	6:mOYOC7LElN9gEHT1Fg9d+9STYfmaj3ckYRlK6t:joPaHfmarcP
MD5:	070D7B361CDBCED2E08F459987E73AB9
SHA1:	E42DB9AD60C61E73FCAD0421BF428ACB72976985
SHA-256:	F9838D256F141C327A1E7D52DDA6D3CB38EC5A6198887C5F29C12F647930335D
SHA-512:	699ADCC2D72270B3626F216C655B3EFA5E1197C9716AD9E2C7CAC6A8E32D93462BBFE76CD9E4D0FC9616C3D403A058B4CCD899BA278197CB2D13DA133109E 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05fcd8b85e1b3284_0	
Preview:	0\r..m.....T....q....._keyhttps://zix.com/libraries/bootstrap/dist/js/bootstrap.js?v=1.x .https://zix.com/...../.....#.....>.Hn$j.....>....<S.X.....2.A..Eo.....k.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0732e770b7a445ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23898
Entropy (8bit):	6.068760792409269
Encrypted:	false
SSDEEP:	384:coIXR+JpnUXkC/hn9bWA5aGOHpYDTYWYlbnEo/9mTCVNlEOlF/XVCrAJYUTy50t:NU06l+aqS9mTCV0o3t
MD5:	0E727182C2F20AD98909C25B93BD5AAE
SHA1:	1AB9C3292D2D54255511EC36FA855F543043DC4A
SHA-256:	5B0E20966E092EA955D21C49ED05EF4D4FA600299FC487A0347417FDC8EB3076
SHA-512:	E51A0E6CB1EFB0FDE2DB7011FF7691B98656A64A27F93AA5DCE547702EDC98B92D6E43DB8467042F080BCBA20F084AB1AD6112C75256FBB6DCFE2565E1F5809
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....0...._keyhttps://js.driftt.com/core/assets/js/23.5562c7f5.chunk.js .https://driftt.com/B.V.../.....=.>...l@^..^..1..o.....A..Eo.....V.....A..Eo..... .....'..E....O.....[.....*.....x.....(S....`n.....L`F.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.... ....`.....a>.....Qb...}....I4WpC..Qb~.s.....luzPC..QbB.~.....JhcMC..Qbr.k^....KA4JC..Qb:.....MWt3C..Qb2VM/....PGb/C..Qb..\.....UXBQC..Qb..oS....dZmzC..Qb..H..... fTFZC..Qb..A.....jKoDC..Qb.x.....pgTpC..Qb.....tGI+C..Qb.&c....vkRnC..Qbv.Q)....xyhjC..Qbj.Q....yAzeC.(S.$.`....]..K`....Dc.... .....(Rc.....1.`.....Pd.....push.I 4Wp...a.....@.-....HP.....9...https://js.driftt.com/core/assets/js/23.5562c7f5.chunk.js...a.....D`....D`\...D`.....`....&...&....&.(S.$..`....]..K`....Dc.... .....(Rc..... .....q.`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08d63749a47a6a6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	62318
Entropy (8bit):	6.039800378287978
Encrypted:	false
SSDEEP:	768:6wQ+8lfqxXEmUXFRB/8NNC82Fgks2GJQjLuWo+tOi9tmhBMkM68+qVShoLBStuJX:6w18lfq+GyOmFGBMHvnGQ
MD5:	8D0EC4445234886165E84B0FE542A358
SHA1:	49528BDDF99428D6733E74557C950ACD00C8CED1
SHA-256:	8AAADD1F2D4AB1F3B3A6BF653645FBA4E4BBDA0A0D29A4A8AFBDE1C9ADC2C01F
SHA-512:	63048AFA25744B6CB921587F91E922FD12CD0C0F0E30C45D60F3FBCAB8792BAF18AEDA68DC240EDF22865D8C8816240E8445ED5A1E5C4F5537F97522CFBF78A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...2./>...._keyhttps://js.driftt.com/core/assets/js/35.9da4441f.chunk.js .https://driftt.com/LyC.../.....Q4P.j.(..y.T.9....\.z.....A..Eo.....r.....A..Eo..... .....LyC.../.....Q4P.j.(..y.T.9....\.z.....A..Eo.....M.....'.0.....O....`..."X.....(S....`..... <L`.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....F...`.....,.a.....Qb..A.....A5mOC..Qb.....KrFpC..Qb&;.....UM5qC..Qb.....h E+JC.(S.....`.....L`.....y.Rc.....QeB..t...._slicedToArray... QfN..~...._arrayLikeToArray.....QbFd.....r.....M...Qb.`.....o.....S...R....Qbv.....s.....QbRF .....f.....Qbv]..... m.....Qb.f.....y.....QbzG|.....p.....QbN.h,....v.....O...Qb.-.q....w.....Qbb+.....k.....Qb...&....z.....Qb.....O.....QbF..)...._.....Qb..Y.....j.....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a410274e64860bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.511207862506839
Encrypted:	false
SSDEEP:	12:M//TIwvDvlPWW//TIwvOquZ7W//TIwvCttun:MXTIQRPWWXTIQOquZ7WXTIQCttun
MD5:	534502B33BC7AD8E50F229AAE1E7A587
SHA1:	987A64A9D7A02AAEB8EF725ECC22048BB3A664B1
SHA-256:	5622AECEA19BAED7331CCF36783B90CBEB16046A7F355354B5F4952DE748E071
SHA-512:	160990BF4BEB9A882D2081E3CCE2C38262A8445AAFF8FE5D44E9DBB83918E5A41ED89DE9A1ECAD0DADE0505D9AD40F5627DFE0E43CA3EA04C96B9642044C47D1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...<....._keyhttps://www.google-analytics.com/analytics.js .http://eriglobal.com/...../.....<."....F..;J. ....6.C8..phG@.A..Eo.....dh.....A..Eo..... 0\r..m.....H...<....._keyhttps://www.google-analytics.com/analytics.js .http://eriglobal.com/...../.....T.....<."....F..;J. ....6.C8..phG@.A..Eo.....-^.....A..Eo..... .0\r..m.....H...<....._keyhttps://www.google-analytics.com/analytics.js .http://eriglobal.com/...../.....h.....<."....F..;J. ....6.C8..phG@.A..Eo.....>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e3296782ad5e5d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.588479064066028
Encrypted:	false
SSDEEP:	6:mOWXXYvI5sPXDY4LzW3lSxl67tW7snoK6t:nWRsPXE1hMB
MD5:	3FA566E1F0D3990100BB8049967410FE
SHA1:	46EC133EE5101C60206C1B91695E93C0DEC2F221
SHA-256:	E9E0EE06CFC59517B9D9C6633A13CB9B0F8C120C788560EB484B596ACBC69909
SHA-512:	540F113AAC5C7272D5F7EC63CB742D9689CDEF3B8D75C4B14E9A0AF60C1428765101A7AA72BB2486F162CFD56B53825E3CCE0B9E1B503C759B9AAB303E2812 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/fieldvalue.js .https://zixmail.net/...../.....Si.....&,...q....%..X./..i..F.d..-.JE.A..Eo.....1&;.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10cf6fd86d883fb4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	30772
Entropy (8bit):	5.795953853671907
Encrypted:	false
SSDEEP:	768:dL1o1F//+c9l8FA7ams/wc5luMoF/vdjjpyz:dJYN/19lI8anwYsMaFjjpyz
MD5:	D86870D0AC2D93DF9271CA85418E932B
SHA1:	739C227F9A82BD49CF2BFEADF7A4EA2BCBF5F133
SHA-256:	03C69AD85E7B1E2E3DEF5A21013B80FDA8ED861D20DEAAF1F6ECC248B4E6CC89
SHA-512:	950A71F583F0AAB8B9A73D103BD13CA3539DBFACB870A86205CD0B55608665961D12B11DB9BF752C6B33D6D557206A1670840744AE35E455285D24BA07EB27A(
Malicious:	false
Reputation:	low
Preview:	.....'..C....O....xw.....(S.l..`.....$L`.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....V...`..... ...a.....Qb..XV....A/QlC.(S.,.`.....L`.....a>.....Qd&I.F....attachment...$.a.....Qc.,.....error....(Qhve.p....Failed to upload attachment...Qd..mJ....errorSize....,Qi.....File must be smaller than 25 MB...Qdz.....uploading....(Qh.!,.....Uploading your attachment.....Qd.F.....automessage....a..... Qfnu`.....emailCapturedSuccess.,Qi... ...Thanks for submitting your email. Qf.....emailCaptureMessage.....U....^a..~...H.e.y. .t.h.e.r.e.!. .W.e.. r.e. .e.x.c.i.t.e.d. .t.o. .h.e.l.p. .y.o.u. .o.u.t... .L.e.t. .u.s. .k.n.o.w. .y.o.u.r. .e.m.a.i.l. .a.d.d.r.e.s.s. .s.o. .t.h.a.t. .w.e. .c.a.n. .f.o.l.l.o.w. .u.p. .i.n. .c.a.s.e. .w.e. .g.e.t. .d.i.s.c.o.n.n.e.c.t.e.d.....Qc>.u.....composer.,.a.....Qcn.....footer.....a..... ..$Qg~.%.....me

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11c9e752de6044e2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.820008114510955
Encrypted:	false
SSDEEP:	6:mjEYZDtVcmWyJzJDx/SlEbQs/m4fllZK6tB/SHHEbQs/m4C4z0CH0msXWnL9BEbF:eVx1zVZsRs/fllTz2Rs/x0XNGnRBRs/
MD5:	3CA41FC8F95E4782BCC78EF31F3E9AD9
SHA1:	51DBFFB50B696D377E8BE18B4BE07F9C5AE6E325
SHA-256:	C7223EC25242C33785360B3096C0054B94EEB7729B125DF0A3594398A8013F22
SHA-512:	A0F22AFBB77B759FF7A14BC1C4F049BA8AA2B4E07BD951093D5BE07147357829F62D6ADCC2E59DA0FBF387A856F39AD1F0118E80B430875E1E5210597DD5FEE F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...@..6...._keyhttps://js.driftt.com/core/assets/js/8.b94e6c9f.chunk.js .https://driftt.com/,}C.../.....ji.,...h.?...z...?P5..\...h..>..A..Eo.....7.d.....A..Eo..... .....,}C.../.....".....ji.,...h.?...z...?P5..\...h..>..A..Eo.....2nA.....,}C.../.....4962C93E08307FE133B6A71B47C0E108273387CDB90291BF5F54923BFC325E8B.ji.,.. .h.?...z...?P5..\...h..>..A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c5861241d6b406d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	59414
Entropy (8bit):	5.69667842787487
Encrypted:	false
SSDEEP:	768:Y8NlLiXVOJoNTcOTbTjSk3EafI+BnUJgl6R6m0Pvm0OAlt8Hw+k:Y6LiXKoBcWbaKIgRc8jBdT8Qd

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c5861241d6b406d_0	
MD5:	1B101906FA2EECCE432D1194E0FEFAB0
SHA1:	30CA4FE29A82A42931AC3CDAA7269BD76A5611F6
SHA-256:	6E755820F944BF37E76403C1AF35D3125616C56BBE15142CDFE084C42B005CD7
SHA-512:	EC2A5F2DAD4277465619CD079A205C0EEAD65F673056A87E6E7C20BF8321B51CE9744A1410C0F8DA247F55C0F1D3266074D9F963FB36893DFE5B782A7507EE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....h.{...._keyhttps://js.driftt.com/core/assets/js/22.c3832689.chunk.js .https://driftt.com/.vC.../.....W;*...Z. nT.P.k.lxZ.....n.A..Eo.....Y.K..... A..Eo.....vC.../.....W;*...Z. nT.P.k.lxZ.....n.A..Eo.....:y]l.....'.....O.....W..... (S.%...`.....L`j.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....,..`.....ab.....Qbn..y....1FNfC..Qb.....26VMC..Qb.c>b....5CQLC ..Qb...S....AHQfC..Qb.J0.....AHYTC..Qbn.....IZJCC..QbJ.....IwrgC..Qb>.....MiOAC..Qb..'.....N7nIC..Qb..t.....Nx04C..Qb..Q.....VKa5C..Qb...j....XywmC..Qb.....bTzNC. .Qb.....cJHJC..Qbbf.....e9BDC..QbN_.0....exJpC..Qb.La.....h5q0C..Qb..UH....jiYPC..Qb.....jniCC..Qb.(~.....mekdC..Qb.~.....sY30C..Qb".}.....u77mC..QbJ.....xqFTC..Q b.f.....zgdOC.(S...`.....DL`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20649622586617ff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15898
Entropy (8bit):	5.772878610334888
Encrypted:	false
SSDEEP:	384:EBFZ8ran4Q2d7UFlzpq+24+Wc5Xvr6D3ziR0ljApsTX6taPNdGG:nDCpT+XAW0gnT
MD5:	86C38AC4144BEDB230ABF040F2D591EF
SHA1:	B98A1CF62314B198CAD000B62E3CAB4A82B0FFC3
SHA-256:	7D8A9CB0097674561D8F69952D33160465A59556D3374E343818E5E6AF70243A
SHA-512:	E6E9B24363C8622B086340EB741BC76D9986DECC74C456B09B42DAF77EEA13209FD6B4A3C319180241129BC92AACB4C21B077C66C34AEEFD2466425266B6ED B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...,....._keyhttps://js.driftt.com/core/assets/js/17.0833007f.chunk.js .https://driftt.com/h.V.../.....iz..>N..o.Jk....\....._.C..A..Eo.....(.g.....A..Eo..... .....'..@....O.....<.....?.....|.....(.....(S.....`.....L`f.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma...."...`..... .a^.....Qb..o.....+GZiC..Qb.*.d....1Z3aC..Qb.z.W....8ZCyC..Qb..u....9HpmC..Qb..Q.....9wXnC..Qb.".S....BY8AC..Qb."(S....Jrg8C..Qb.....Jwn2C..Qb..X'....Mur8C..Qb..... ..NJA7C..Qb.&.....Uo75C..Qb..2.....Y0woC..Qb.0.T....ZtgxC..Qb...%....oY6KC..QbJ.....pYxhC..Qb.[."....rmQ0C..Qb.4.....slYPC..Qb.....sxX9C..Qbn.....txDsC..Qb^.D... ..vYbdC..Qb&Kd.....wW9OC..Qb^.O.....yT62C..Qb...d....zoZMC.(S.$.`....]..K`....Dc.... .....(Rc.....1.`.....Pd.....push.+GZi...a.....@.-....HP.....9...https:// js.driftt.com/core/assets/js/17.0833007f.chun

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2147111f92e1d00b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	392
Entropy (8bit):	5.561391453304337
Encrypted:	false
SSDEEP:	6:mZnY0Za1CollSdBHt/rvJhK6tWZnY0Za1CBaS8mtWBHt/rVZK6t:ofZaLlCBhpafZaVVmtWBnT
MD5:	73C3BBF75E6C55A33965640156A1BE0C
SHA1:	C5E8AFF939086156994C60E5055D9D9D71647820
SHA-256:	47026609C6A6E48FA48160109473115BAF97065EADFA3EE614BFF48DF728E0D2
SHA-512:	576F1F6586DD3076890EEA1784F847C01B07842B378376E3FB7300843D4DD2F306E4915F11F468CFE3573B89C1A81A38D7AB2AC49B1248F496D3895403BF5F95
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@..."....._keyhttps://tag.demandbase.com/14fca94f.min.js .https://zix.com/...../.....t.....HQ|..[..K9.,HI...+.....3!.\.A..Eo.....&G.....A..Eo.....0\r..m. .....@..."....._keyhttps://tag.demandbase.com/14fca94f.min.js .https://zix.com/[{..../.....%.....HQ|..[..K9.,HI...+.....3!.\.A..Eo...../u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\218586790dcc80fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	70296
Entropy (8bit):	5.825957046990548
Encrypted:	false
SSDEEP:	1536:01YniQksCCvyjjNTsWUbxKKkl0uN+ILgw/PP9z1S:RoG2NTBgA/8ILPP95S
MD5:	E112146C86B15BFC44D4B5D9FA725A4E
SHA1:	A28C9B956FF729F25C7EB8CC0B85219AAD4C4F13
SHA-256:	DEAF6E282ADFB583A1ADD7493B99E6C40813AF7AD822AC00D6F779A794767AEC
SHA-512:	69B7A67EF588FC39DEEC16D6DE4ED4596611558ED77B49EF9A4596C08FF29B1923F5DCCB640EC24E6A80D7A5AFDD509B8A755C4306CED49A957EC87889D5BI 00
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\218586790dcc80fc_0	
Reputation:	low
Preview:	0\r..m.....@...v.....26106C09CFA41A7052C57DD4620BEE069F46C5132AABF9CA4B1DE4AAD3397753.....'.....O...`...I._..... .....(S....`>....|L`:.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....:...`.....I..a2.....Qb.UZP....F63iC..Qb~ .....JBtmC..Qb.9.....JygxC..Qb~.....Lm5sC..Qb*."."....WSu0C..QbV.....aY38C..Qb.z=....bZ7kC..Qb.....maj8C..Qb...t....prCuC..Qb..f....r/K9C..Qb.....ssRiC..Qb.0.<. ...zHZoC.(S....`.....L`R.....Rc@.....QbFd.....r.....Qb.....t.....QeJ.....defaultSetTimout. Qf.o.....defaultClearTimeout...Qdzg6.....runTimeout.....S....M...Qbv.....s..... R....Qe.L.....cleanUpNextTick...Qd..2....drainQueue....Qb..V.....Itemk.....`.....Pd.....push.F63i...a.....(S.....Ia}.....1.....@.-....HP.....9...ht tps://js.driftt.com/core/assets/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\23aff70ab1c25091_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25314
Entropy (8bit):	5.825314772417094
Encrypted:	false
SSDEEP:	384:dqmT+KEV5A9xvN4crsBTHGMTwCK1IqmT+KEV5A9xvN4crsBTHGMTwCK1m:tT+KElFsBTHGg5T+KElFsBTHGgj
MD5:	8ECA6FC95EB70EBF5EFEA017CCAF9A3C
SHA1:	AF618FD201B6783663BE6699F633886CAB9B37C1
SHA-256:	27434B301FA5AAAF901D69C52FCF480FCA2B7319C351C5A07FC39A9AD7193C91
SHA-512:	C869970D545D7A9EFCF0D302C9E61C69D1BBEBBBCD1DAE22F3F9D2300DFE55C9BD19BF763F24F4E06AF161721B87AA312DAC82D45D88E050FF678ACD60A70 2E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...U....._keyhttps://js.driftt.com/core/assets/js/32.24776eab.chunk.js .https://driftt.com/.JP.../.....wd...[.7.....6.$`:.....OS....A..Eo.....g.....A..Eo..... .....JP.../.....wd...[.7.....6.$`:.....OS....A..Eo.....w.....'.....O....00..t.PT.....(.....(S....`.....DL`.....Qc.....window....Q.P. PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....@...`.....4..a.....Qb.e7.....HSQLC..Qb.....SkRIC..Qb>.....V+70C..Qb..s.....V4ETC..Qb>l[.....p2bkC.(S. .`H....HL` ....`Rc,.....M...Qb..F7....c.....R....Qb.`.....o.....Qb.,(.....l.....S...Qbv.....s...f.....q.`.....Pd.....push.HSQL...a.....Qbv.47....d.....(S.(. `....]..K`....Dd.....,Rc.....l`....Da.....@.-....HP.....9...https://js.driftt.com/core/assets/js/32.24776eab.chunk.js...a.....D`....D`D...D`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\246397e51840c87c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.614855727746435
Encrypted:	false
SSDEEP:	6:mKVYvI5sPXD/ajWFVgM0Et9lSBeEa9H4RrbK6t:dsPXTaqFaEtHCaC
MD5:	25BEE9209A00CDB1807DE0645B01330A
SHA1:	E128E09D35D029C4DB020D00D6DEDD41985CAF8F
SHA-256:	8F5B22F466DD58D2D2D757FFEFFAAE251008EDB12F996737DDDA0D35656FEC0C
SHA-512:	4B7D05E4DB06499F9D8388771E0E64E57EED8035470656D7D621EF2A2F4F9A43A7AB9892CF587CA60DE965CEA75C0DA6A99A0D1E0D6A975C49A50EF89F3FC2 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....#...._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/scripts/jquery/jquery.js .https://zixmail.net/...../.....l.....7.`D...'x..R4N..{aY* ....,..9..A..Eo.....@.Gi .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24d7281d94368b01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.528488210090372
Encrypted:	false
SSDEEP:	3:m+liS08RzYOGKXcmWpgXVkdaThtF8+9tlHCkHmta7oz4mq6tlpK5kt:mFSVYOGMcmW0VDTjn9SOSa7YLK6t
MD5:	9C7372ABABDCEB2ADD7609CEBD7D9951
SHA1:	3494C070F3726C5B96569005584B0E15EA58E578
SHA-256:	FEF78B9A23BD57864ACFDF4F106F672248EE0704E5C36B6D7B170554F873FF84
SHA-512:	3A0B6B2DF4BE300C28CFE0360099749268687429 3E51CE3028CDD91C8CB73D4C24365E520DCDECD996EFB305EFD2ABEB324FCCF5635BAC362A4AAD67F3743 DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://zix.com/core/assets/vendor/jquery/jquery.min.js?v=3.5.1 .https://zix.com/...../.....".....r.@%x:.. ..".F!42.j@9.....A..Eo.....-..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2963110023e01e19_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.439955720901946
Encrypted:	false
SSDEEP:	3:m+lyvF8RzYOGKXQTqD3t3atlHCjClU4UI7LJaQCm6gK5mJh5X/pK5kt:m4YOGMQTqBqSjCW4QP4JvXhK6t
MD5:	84F37D11E566BD89FF09D161E01BDB18
SHA1:	7FD4AEE964BC0BC40495DB8268C658099CCD9E77
SHA-256:	CD259D32A786E01212340FBA4F46DEC4BBF4679AC759552FD99E46AA94D34F67
SHA-512:	C340C779322EE1F0C72623CC44BB647D6B62AB301436340B47F8191665125A8958D2559D7A2C0A39D7BEDDB7685C7BB32F6F4392B55C80AFF3D513704422B973
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B....=v{...._keyhttps://zix.com/core/misc/drupal.js?v=8.9.10 .https://zix.com/...../....."".....P..x...S...9..#._.....3G.u.;...A..Eo.....0,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a2e88f45b19464c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96392
Entropy (8bit):	5.825956165666481
Encrypted:	false
SSDEEP:	1536:iju3QjQdNvUGiZkHrugwuoaqSr0yXyewkFnw5O4Q:xNMErugH9iiFnw5Od
MD5:	A6173C20207A1E04065E05B4D8EBE8AD
SHA1:	CB22BA2DC6675D7F2CFB7B622BAA01D6DA90E134
SHA-256:	A558B9B43C741DFAA21901C5F04CD26DCD1D06AD264DAD4A6B7A383B7EFA4B73
SHA-512:	DFF6430EE767E884DD6220AC983A90D9EB3BB50F19482145310A3BBF95CDB916174B4444D12366CB028FAFB960D0B4B87E09EA304883D200379DB74C490A17E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....D6247ADC89A02974E028021BCAB45C2A6A79E5753E94B8B9D7447CD6C1E81633.....'..S....O!...0w.....`...H#..... .....,.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb..q>....t...`....I`....Da....j.....Q.@.....module....Q.@>`.....exports.. .Qcn..*....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....8P.....+...https://code.jquery.com/jquery-3.3.1.min.js. a.....D`....D`,...D`.....Y....`....&...&..!.&....&.(S...I#..`FF.....L`.....Rct.....2.....Qb.zgt....e.....Qb6%.....r.....S...Qb.4.Q....o.....M...Qb.....s.....R....Qb&}.....I.....Qb~. .....c.. ...Qb*I.[....f.....Qbj.....p.....Qb.....d.....Qb.4.....h.....Qb..R%....y.....QbNh.....v.....Qb..E.....m.....Qb2T.a....x.....Qb.....w.....Qbf.....T.....Qb.S.....C.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2facd160e9b3281d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7466
Entropy (8bit):	5.894764112575213
Encrypted:	false
SSDEEP:	96:y9D5WKg2hWMoWXFeLAMYu8R2lgb4ie+T6C5tkU4IrG9TNk3QfGlYs8+s9OMqMyZq:yWK1BIgu8R25SptkNJkFITY9OZnO8JSr
MD5:	1A69E272CE3C9EA972917355E0D11845
SHA1:	73C46EAC2D05CEC992996527F4180E12AF512BFB
SHA-256:	98B3A593307ABEBD59846B9F28BDC4E57E5A7009C9F16936F0D82D02388993AA
SHA-512:	9DC8F9E84342B4D6CB2B07909AA2F43D6BF75790E35D50D680A5394EF4E7201E8F38CC15E7EABC782D29B9FE4C8385F16D7C815993C44ECF2841D80228A872C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://js.driftt.com/core/assets/js/31.097eee16.chunk.js .https://driftt.com/..S.../.....p.....G...P.f..D0.....r.+;....c1....A..Eo.....A..Eo.... .....'.....O.....,A.....(S....`.....LL`".....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push....`.....L`.....`.....Ma....>...`.....<..a..... ....QbR.`.....2AO3C..Qb..v.....HXmnC..QbF.W.....My8UC..QbR.....RqwxC..Qbr..i....VSUxC..Qb.....yhQpC.(S.e..`.....dL`.....RcD.....Qb.....t.....Qb..F7....c.....Qb., (....l.....S...Qb.`.....o.....Qbv.....s.....R....Qbv.47....d.....QbRF ....f.....O...Qbv].....m.....QbzG|.....p.....Qb.....O...l$.....`.....Pd.....push.2AO3 ...a.....QbFd.....r.....Qb... ....mj2O..Qb.....n.....Qb..e.....7SM1.....Qb.k@.....QtlZ..Q...Qb.....ERkP..Qb.5.....uDfl..Qb.....SkRI..Qb2.h^....7oto..QbJ%_.....C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fd021f1c66e0410_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	59394
Entropy (8bit):	5.768712228644002
Encrypted:	false
SSDEEP:	768:jZMJ3bums6na0bLnsrUvEbWJRPEQFUN3QUbv3aiki/lpq0SGQNY39V0bN4:jGrums6nvHscrFqqMq0SVNYwN4
MD5:	8A2E8BE00B87D1D1DB2ABAB3EBFEFE21

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fd021f1c66e0410_0	
SHA1:	175812C5230A288410E9C71A82E8CF06A8B419FB
SHA-256:	D6D69760BBE2E092644B5836A9F8A16D55D705EFC1C301820C15F2D33DD175E9
SHA-512:	BB1772B0C0E63B42ECD3E59C2DA464B41942625CEB4015A335D88D8CD57C64E945D84A4478F2E4044D2862443D73F54DBC34D9228DB823B486A56CE9BA6764E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....+...._keyhttps://js.driftt.com/core/assets/js/28.a2bddfe2.chunk.js .https://driftt.com/|.T.../.....t.....8$.l$t7.b..z..7...{.....DGA...A..Eo.....aI.....A..Eo.....'.....O....H....].3.....<.....X.....(S....`N.....L`>.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb....push.....`.....L`.....`.....Ma....8...`.....t..a6.....Qb...Z....3fZ3C..QbF#.....3kqRC..Qb.....7VeVC..Qb".z....Gzp1C..Qbn24.....ILS/C..QbF.....LaGAC..Qbf.k`....QkD hC..Qb...*....W+sfC..Qb.....gf09C..Qbb.....oPI6C..Qb".6.....pqMuC..Qb.....uiOvC..Qb.o.-....utatC.(S.<.`2.....L`.....0Rc.....QbFd.....r...`.....q.`.....Pd.....push.3 fZ3...a....L.....q..(S.....Pd.....e.exports...as.....I.....@.-....HP.....9...https://js.driftt.com/core/assets/js/28.a2bddfe2.chunk.js...a.....D`....D`L...D`.....`....&...&....&....&. (S.`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36211ac3aab3f4f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	441
Entropy (8bit):	5.849906934494276
Encrypted:	false
SSDEEP:	12:1J/SVxi3GuVPypuGs/tNnuGsG/vLqcGwW:1J6VafPsub/t1u9GXLZ
MD5:	572759F749E6F13E12EA4D959F55DC4F
SHA1:	58B95DFCF64F7D1846AA8217EB04F95BDB8D963C
SHA-256:	5A8AC593BE090BDF6100E226C97F320D9BD52C84E86571A58C1DDD94CD1961D2
SHA-512:	32B919216B65701A33B4BE5F2B90BC6A15788C186F4227B12B1CBF9EC7F266C77711140F401D540B90287FFA0CFDF430784636F54CE4E270E7DCDDC38625DEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...=u&....._keyhttps://js.driftt.com/core/assets/js/main~2e35577e.69c90f86.chunk.js .https://driftt.com/..C.../.....$....._4...;...p..{..@..h.Y...b.:.A..Eo.....H`. .....A..Eo.....C.../.....'....._4...;...p..{..@..h.Y...b.:.A..Eo.....P^p.....C.../..Y..B07F18CF8A68AAEC8027A590EA8474DE510B3905AA3804552AAF254 8973FDF03._4...;...p..{..@..h.Y...b.:.A..Eo.....nE.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b38794615c80537_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	87176
Entropy (8bit):	5.86758729081276
Encrypted:	false
SSDEEP:	1536:aM8NbXsixKQPb4aGg7NQMNvtzF449+iAQHyD8+g3c:gtfxZbrGRMNlQiFHrc
MD5:	23AC189AE7C1F309CACC1513F5A24BA3
SHA1:	0D36883CE1738F404E29A2F27E0FA401A9E32909
SHA-256:	2752B1A22C9BF671CFDFEC52B1AC89F9968A5842B4B5E8CB0653599D59B9ACFD
SHA-512:	3B83CF4114D705AE9B2973355E2E8170191EF1EF6BBE8DB5E27148C4C3D44F5C6CF7AFB63ADD23E8F2F41BD73454B7CB313DAB82FE4A73F624B5367FBA56E3 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...`0f.....04ABF84D50FEA6A92A7CDDC2F91E622A2E4AC93D4C2A3AF2E840058D8413BEF9.....'.....O....@S..TIG(..... .....0.....(S.U...`^.....L`.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.....`.....a.....Q b.|?f....0zX2C..Qb.4.....1FobC..Qb6."....1J7aC..Qb.1.b....1TxVC..Qb.r.....2JD1C..Qb.....2jbgC..Qb..[....4+fuC..Qb.;.....4GeQC..Qb.. .....5aO3C..Qb.....6BARC..QbzJ. "....7Ru6C..Qb..e.....7SM1C..Qb.H.....7jL2C..Qb..D.....8dj6C..Qb".j.....AVLeC..Qb..R.....Ay6XC..Qb^?.....BP9pC..Qb.N.....BtTtC..Qb..&....E7j9C..QbN).....FYayC..Qb.A.. ...GmLwC..QbR..q....IOASC..Qb.....J1qwC..Qb..A.....LvsCC..Qb. .....M44JC..QbJ.....O3AJC..Qb*.EQ....P0jVC..Qb...U....PeZKC..Qb.....Q2eFC..Qb.....Rl48C..Qbz..*.. ..SoalC..Qb.S.G....TVvmC..Qb... ....U57QC..Qb..fv....WBY7C..Qb...;....WwEgC..Qb..P.....YsDtC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3eb2d54d6b1ecd70_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.575677034235423
Encrypted:	false
SSDEEP:	6:mmpsYvI5sPXDaAWEsxGL9lSwv3tiZK6t:p6sPXzsxCD3o
MD5:	0D99B1C61EED8E0FF8E8B10CDFDC1A9B
SHA1:	9A804C72E1C26CEFF4EFCA8DDDA5AFD068A3F713
SHA-256:	4A2B9671BD0752FB4CE6FD34CC4A4B173DA3E07747135AE6DC7314846B1D83A0
SHA-512:	A312AAF83FF817EB419F42126DD57697A2AB584415EF026250164442ACB8A9187302680310DB653504742F52CC83A22848CFE72334B3684A44A0EC915BB3884B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3eb2d54d6b1ecd70_0	
Preview:	0\r..m.....e....V....._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/default_validatorconstants_en.js .https://zixmail.net/ax..../.....h.....?..O....D..k...t...]8..j.gR>..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41475b42dddb0b1b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.479321672821224
Encrypted:	false
SSDEEP:	6:mi/VYGLkHRz6+MEQT1F7SB/Y1hvL1lDK6t:ZEZQTrYw1RL1
MD5:	E6F639834BD7D7E65513A0B49CFD2DE6
SHA1:	D99B045780A8DF39996B5813859521F8F82591F5
SHA-256:	373C324F9D5CCEAEC1DC57C4C21486E64CECA7BACC87B9EACEDF108CAB354CA4
SHA-512:	E70FD79C2C1FDD137D266C5E4CE15F030CB45AF5B191CA968FDABCF23A8E665AA8744672BBD433315A7D6D0E619E767EA6D25DAC0A710E163CCAA6FD851510C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...Km[...._keyhttps://www.zix.com/themes/custom/zixappriver/js/main.js?v=1.x .https://zix.com/.'..../.....{.....J..K.a...xR..t..Ve...(.....+.A..Eo.....qV.%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48367205b83f4fa8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	58357
Entropy (8bit):	5.694656823106775
Encrypted:	false
SSDEEP:	768:nFhYw9SUn7JR5AwQXtrZhiQq6kgqx26IT96Nux:Qgn7DiwyBm5gvj0i
MD5:	4FEA450A798EF6889B261547299B6F50
SHA1:	59D7C0B32AD86942BA728D62090F3202AD2975C1
SHA-256:	F2B45139D940FB2814602984F20D0358BE7F747DD6D5F5C4C10D4116046063E9
SHA-512:	A6EE97B429560689E3A03873C191F15CEE2AC4329C4DE9FB9E65EF6140B2FF084559F8BF1E2B2BF49C5E08112DA7F8E8D3198137517FDE7F6BBD93C4ACDE0546
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]......y...._keyhttps://js.driftt.com/core/assets/js/main~53ca99a6.4d7f7a8a.chunk.js .https://driftt.com/C.C.../.....;.z.th.~.....X.@..-....|P..A..Eo.....KeAi.....A..Eo.....'..f....O....8.....`.....D.....`.....(S.....`.....L`b.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.....`.....`.....L`.....`.....@Mn.....L...,.....:.....F...B.....aZ.....Qb.....+ZvlC..Qb.....0lfvC..Qb.tqV....4c+FC..Qb..Q.....6lNaC..QbV.....7BJgC..Qb2.h^....7otoC..Qbz/.....8saYC..QbFi.....9xv8C..Qb6.o+....BMKrC..QbJ%_.....CpupC..Qb..q....EQxiC..Qbv|.....F8vJC..Qb.n.....MFhOC..QbrW^.....NletC..Qb...3....PjZBC..Qbf.....VYE+C..Qb.J.2....gG69C..Qb.<1.....l+XeC..Qb...3....moLGC..Qb.....qeWUC..Qb.-t.....t8dsC..Qb.....wNJwC.(S.X.`f....$L`.....HRc .....QbFd.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\484a67f8e93657dc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18185
Entropy (8bit):	5.723077821441938
Encrypted:	false
SSDEEP:	384:iCEZEjw6M0/gFC61cGt5bjdlxA+OM8jKXXSNo3e5B8bj0NXbF:v/M+/LGt5HWM8cM
MD5:	AFD830CEE3A09919956CEDFD6EE0A10B
SHA1:	841BCE129E7A5D9DA44996DBD758F505108D89AD
SHA-256:	BC083C3C180BED1615C7C2A8857DF231C75C3D8A9C1E001B7A985002084B70CA
SHA-512:	612DEDEC8E2188BF7BD6007CD07374BC96B71CC5285978C1D4C557A6B70B2DB571B2372BAA1F081837A10E9158A0C0E11637419F02989DCA87DCC360C612423
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....}....._keyhttps://js.driftt.com/core/assets/js/1.0af467a5.chunk.js .https://driftt.com/..T.../.....s.....+W....i.;...(.@...._$.1.h..A..Eo.....{.....A..Eo.....'.....O.....E.....h.....(S.5...`.....L`r.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.....`....aj.....Qb.....1KJDC..Qb..L.....5rQpC..Qb.....5utbC..Qb2..4....AZnIC..Qb..7....BDBSC..Qb&!.K....E/MNC..Qb2.....F5GSC..Qb.s.....FWHKC..Qb.K./....H0DWC..Qb.Y.b....liFMC..Qb^!W.....TVEOC..Qb.<C....Tr4LC..Qb..KH....WL9lC..Qb.I.....aoSQC..Qb.O.....d5gMC..Qb.....es7IC..QbV;.b....gnzxC..Qb..>-....liE7C..Qb.fi.....lzB5C..Qb./\...nGxMC..Qb.5.....nkkXC..QbzX.....o+42C..Qb.1.....qNv9C..Qb.W.....snMeC..Qb.;fy....wAvlC..Qb&.....y8iBC.(S.,.`.....L`.....(S.....Iav.....$Qg./....._iterableToArrayLimit...\.@.-....DP.....8...https://js.driftt.com/co

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d8b7a5ac3fa9c09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d8b7a5ac3fa9c09_0	
File Type:	data
Category:	dropped
Size (bytes):	88488
Entropy (8bit):	5.903802379624043
Encrypted:	false
SSDEEP:	1536:GQLY4Y46rv9Q/fZmAWmMopTCXYksxIEX0sspn39:NCD9wfPWcgTsj0/
MD5:	57AC8EDFF3DF0E2E9336B1568AA5ADEE
SHA1:	15196FA4C712F9925F767233B99D439609994214
SHA-256:	1FFC831F5A2565AD3439AB2A720CDE2CDE3CB343317B525FDCCE3A4B717D1794
SHA-512:	67A82EB9312FCF34B5650665A5AE81E6F613A3AC5394DA599FB3B557AC9ECEF86A029E5DEFF5806240FBAD615EB289E029409807685259049 8B61613E43CE57C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....b....B07F18CF8A68AAEC8027A590EA8474DE510B3905AA3804552AAF2548973FDF03.....'.....O....XX..y.....<..... .....|.....`.....4.....(S.%...`.....L`j.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.....`.....ab.....Qbb.. '....+oIKC..Qbj.....0g5bC..QbN.....1tbhC..Qb&..w....2XY6C..Qb..L.....8LPeC..Qb..`.....AbXdC..Qb6.....BAMiC..QbJ..4....CYoeC..Qb.....E1gYC..Qb.....FAmhC..QbjP.... ..IpSJC..Qb.....OA1uC..Qb.....X9/cC..Qb...<....da4LC..QbJ..I....g6eDC..Qb..2....jbOzC..QbZ.....pvgoC..Qbn.0o....qwiDC..Qb.....r0JTC..QbR.....sRvkC..Qb.v..... sa5DC..Qb.{.....ws1hC..Qb.C.....z8KxC..Qb*.....zX3+C.(S.-..`.....L`>.....Rc\.....&.....M...Qb..F7....c.....S...Qb.`.....o.....R....Qbv.....s.....Qb.,(.....l.....Qbv.47....d.....QbRF .....f.....QbzG|.....p.....O...QbN.h,....v.....Qb....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\50283a465e0a4d29_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21826
Entropy (8bit):	5.790850933137519
Encrypted:	false
SSDEEP:	384:rnvPbNh15Ep+EC8LOQ9TTOR9YSZXAXNh15Ep+EC8LOQ9TTOR9YSZXAj:rvPbNDc+h8LxTcGXNDc+h8LxTcGj
MD5:	79002DB610129C7B7B7F998FC9041816
SHA1:	4973818B6F0DA720E36410FE14E3ADE8E64DD2FF
SHA-256:	8BDE94AC3BB7FE2756F094A6A41D37BCFB53C35AF5D118C7E527EC8EBF5CBAC0
SHA-512:	291810D812F74582B2299C7D603252892CA859AC0CC5E599794F9551879BCF1FE17BD437869BD06613CB2DF47DD6D720F819C48C44C620BEC4020E6C38EBBE6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....Y...._keyhttps://js.driftt.com/core/assets/js/36.56cefaf3.chunk.js .https://driftt.com/."P.../.....Z...Z...T#-..J.k.....DTc....A..Eo.....<o.....A..Eo..... .....P.../.....Z...Z...T#-..J.k.....DTc....A..Eo.....e.....'.f.....O....`)..|../.....(S.|..`.....4L`.....Qc.....window....Q.P.PM.....we bpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....H...`.....$..a.....Qb.,.....11HmC..Qb.@.....I9iRC..Qb.r.*....wQh9C.(S..`P....`L`,.....RcL.....Qc.!...._extends ...M...QbFd.....r.....Qe6Y.....addLeadingSlash...Qe*..Q....stripBasename.... Qf...I....stripTrailingSlash....Qd.....createPath....Qe.....createLocation...$Qg&..E....createTra nsitionManager...Qb.`.....o.....Qe...!....getConfirmation....S...Qb..F7....c.....QeNp.B....getHistoryState.. QfR..,....createBrowserHistoryn.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\57e301f7a5008375_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.490540008948073
Encrypted:	false
SSDEEP:	6:maBnYGLkHGMcmW0VDTjID/SLWNbxrzK4vAbK6t:FMxJDTo/xNbxzbAN
MD5:	B992F62C9FA0745C0899A1ADBC240F9A
SHA1:	CBEFE638B59123F6E1F1B12BB8B9263B3B80F23E
SHA-256:	A3FA1C77EBB70BE6D1D159C7034766280A84F200F1FF22EEA73717C076EA48E1
SHA-512:	306C1D1CE89C00BAF73BC6FC3D40828BD0AFF5F61EA6B32DED9466356B183ABE934074AD3F7D5146AD0CB676819FB36EB084016C7871A4A5858C66DB9840A9 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y....u....._keyhttps://www.zix.com/core/assets/vendor/jquery/jquery.min.js?v=3.5.1 .https://zix.com/...../.....3...(..z.p.5....`.~b..8..A..Eo..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\61a07f18ec27b798_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.884021211512446
Encrypted:	false
SSDEEP:	6:mkzIEYZDtVcmWyoaQ95JDX/St8C4SFTZK6twK/S/j8C4SFTU6LREQ1rmkhBZK56Q:16Vx8aQXVvwT4SZxojT4SBlrhhB44S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\61a07f18ec27b798_0	
MD5:	7270CF76F4A3E8774AE1C29233470A54
SHA1:	0D3498390FCFC81CB44AFA7C87A58017DBEDE208
SHA-256:	E8ACB46258AC58BCAA11CD4AA8C2901953AFA523ACEF46624B2757223DB6398C
SHA-512:	2DCFFDA53C5BCF6CC4BA2539EB2297107B30DB0D1670CAB7649506D88A94A2F173031D889475A09A9A91D2BD3D28DAC173E46A107BBD7BBCA2652BDC507BF6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....=@....._keyhttps://js.driftt.com/core/assets/js/13.a9247e5d.chunk.js .https://driftt.com/.vC.../.....#....8.g.....q...g.s[..u...z.A..Eo.....X.z.....A..Eo.....vC.../.....#....8.g.....q...g.s[..u...z.A..Eo.....vC.../..S..04ABF84D50FEA6A92A7CDDC2F91E622A2E4AC93D4C2A3AF2E840058D8413BEF9.#....8.g.....q...g.s[..u...z.A..Eo.....=..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\648f965c0b7dabbc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7308
Entropy (8bit):	5.972319265912018
Encrypted:	false
SSDEEP:	96:vUmDWmUPIIJXjwykQsguo6bvB6iMQW9uUgr5pcqXh2KQqYqOQIwUYSQtCPL:XDWvIIJXjwzQob/Qqx/bYqOGD3I
MD5:	37A4C639368B40205C289BC8CF0BFC43
SHA1:	7757024C59D40DA1830DC56BEFCDD8DEBC5318DE
SHA-256:	11C642F4DAC24B7BAAB1805BCD1548F0067247D0EE456BC55632E60652ADE7B0
SHA-512:	2373E0005B10C90F7BBC44743DE9737C0CCF821A0800572541AF287F47F58289505F0A6DED510537279B019BD9B7AC2A17372FCE82C2559636B79CD5569EA2DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.....[....._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://zix.com/.%s.../.....#.9..9h..]........M._....H.].A..Eo.....&.....A..Eo.....'.....O.....(S.0..`.....L`.....(S....`.....L`J.....Rc`.....(.....Qb&}.....l.....Qb../....._.....Qb..q>....t.....Qb.....s.....Qb6%.....r.....Qb~. .....c....QbNh.....v.....Qbj.....p.....Qb*I.[....f.....Qb.....w.....Qb.4.....h.....Qb..G.....R.....Qb.S.....C.....Qb..4.....U.....O...Qb~>OV....E.....Qb2T.a....x.....Qb..Q.....D.....Qb.Y.....L.....Qbf.....T...s.....I`....Da.....!...(S.<.`.....L`.....Y...Qc.M5.....getTime...K`....Di.....&.e....&.(...&.X.....,Rc.....QbZ.....n...`....DaF.....a.....c.....P.....@.-....DP.....6...https://snap.licdn.com/li.lms-analytics/insight.min.js..a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\655aacf938afda06_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	562
Entropy (8bit):	5.868303060579312
Encrypted:	false
SSDEEP:	6:mkEEYZDtVcmWynJDq+aSX+fyI1rbKhK6t+TSDafyI1r/spBcy5WEUSGcjyI1rThA:qVxLVmPfHZq0vfHNdcljH1cljH
MD5:	73C17E744EBF8C387F37DC73EA260D38
SHA1:	9D280DE640F89BDAF88147E87410DF6BB13E1582
SHA-256:	BE615913768BFC3DDB3BEBE101F325F769C7C977D09B156B7B86767CED9438E7
SHA-512:	430BD9A2BCF31B1E5C39EFE5EFC09AF7272ADB0F983F3035172A0B59F11DF3DB5313A73C28521905C47F2B6DF19464087B841479FD444A502123BD812B88DC26
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...1..`...._keyhttps://js.driftt.com/core/assets/js/34.fe729046.chunk.js .https://driftt.com/.#P.../.....I....b.p} r....CP.r.f(.;2.IT3%N.A..Eo.....[.....A..Eo.....#P.../.....I....b.p} r....CP.r.f(.;2.IT3%N.A..Eo.....z.....#P.../.....9134BD9779881D1408BFFC5C3B22B44E0674A996AE084254BB1B7398C6CFADECI....b.p} r....CP.r.f(.;2.IT3%N.A..Eo.....E8XL.....#P.../.....9134BD9779881D1408BFFC5C3B22B44E0674A996AE084254BB1B7398C6CFADECI....b.p} r....CP.r.f(.;2.IT3%N.A..Eo.....E8XL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67ccf06e65d83ecc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114608
Entropy (8bit):	5.7334848310206405
Encrypted:	false
SSDEEP:	1536:1/3dvbIfvoGf7fmkrkDVpKmbFPtp9TyPcdWmhWWWuC5JfQHTzl:11YjWDVpltmcdRhov5VW
MD5:	9917ED16A196B5A644941C70CFA50A6C
SHA1:	1B8B09BBFFC9F4352851992D809294CB7CDE3783
SHA-256:	7A7A332A66D770DC871D770A2C43BA9EE723A330C24E6D203A3199E2B33E696B
SHA-512:	7C2DC23F134D214A2A94E203D8395AC3946F1939B7B439567F2672422F217D221AD5B437CD1A2AB578021D56E5471B0BF7C709832C626571695DD1BD4266DC27
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67ccf06e65d83ecc_0	
Preview:	0\r..m.....@.....4962C93E08307FE133B6A71B47C0E108273387CDB90291BF5F54923BFC325E8B.....'.....O&...H...?.....$..... .....l.....(S.....`.....L`B.....Qc.....window....Q.P.PM.....webpackJsonp....Qbb.....push.....`.....L`.....`.....Ma..... .`.....}...a:.....Qb.....+MLxC..Qb.2...../GqUC..Qb...J..../bytC..Qb.....07d7C..Qb..'l....0BK2C..Qb.....0DkyC..Qb~.#....0GbYC..QbF.....0eefC..Qb.m.o....0ougC..Qb..!.... .0rvrC..QbR<<.....14SlC..Qb..^o....1E5zC..Qb".....27RRC..QbRU!.....2A+dC..Qb.FWB....2oRoC..Qb..P.....33WhC..Qb.....3I1RC..QbV. .....3KgVC..Qb.&.....3bBZC. .Qb.`'.....4BrfC..Qb.Kv.....4HCiC..Qb.....4WODC..Qb.~@x....4XaGC..Qb..X ....4XetC..Qb.-s.....4h0YC..Qb..N....4mDmC..Qb^%.....4sywC..Qb...x....5D5oC..Qb~..... 5DmWC..Qb^..g....5mduC..Qb..9....5s+nC..QbnW.}....5xtpC..Qbr&.....66V8C..Qb...F....6JNqC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7658764de37070f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	651
Entropy (8bit):	5.641799028215242
Encrypted:	false
SSDEEP:	6:mvnYGLSmXZCkyA46lSlnA2rLlDK6tWvnYGLSmXZCkyA4kSHlsnA2rrDK6tWvnYGF:4vyCl6yvy8G01yvy9n7N7w
MD5:	4696BA109D57DD245F56306076B0FC17
SHA1:	41E4DC0244367ED45BDF3A71CAD7E48602F4A809
SHA-256:	375296AF669F9374E8F9D5C4D13ECB1C1B75325624003CBF7818DD0F2923EFDA
SHA-512:	E028760928ABAD8C33A8275F3702A4A833647C3BD0B5B5CBCD835A825A4D586462ABB11587F78748D0A93EFE84FBCB1C649FA0DDBE10828D8CA546B21962F30 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....gT....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-135639887-1 .http://eriglobal.com/8...../.....X.A.C.&."..A\..1.{....o..i....A..Eo.....A ..Eo.....0\r..m.....U....gT....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-135639887-1 .http://eriglobal.com/...../.....S.....X.A.C.&."..A\..1.{....o..i....A ..Eo.....Q&.I.....A..Eo.....0\r..m.....U....gT....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-135639887-1 .http://eriglobal.com/^E..../.....1h... ...X.A.C.&."..A\..1.{....o..i....A..Eo.....o.D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78b25ab234a5213d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	44114
Entropy (8bit):	5.543444542820907
Encrypted:	false
SSDEEP:	768:XpG/MuyHZckghBb2MG53StH6yxhQliQWbOvbhlsIgSVarqkYUDFvy:o/MuyHZrmBb2MGZCSW+hVgSVarqIvy
MD5:	10901AAC645F44B85E6BA8C705600324
SHA1:	42F9E6FF71587ED9D979E06B307E2D28B97ED6B6
SHA-256:	307D9AA808EB67954C577F0B8C3A5E48FE1C4A6F478112C1D536477082BD7AC9
SHA-512:	19DC7D48970B6B9FAAEB4F052563326BF095E0CC4D70D9E8550CB70D8A8B1C3DF35245781213C01543CE052AD73BB8E8BB3D0C4C1BA3B565A65B13F9E300D3 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....s...._keyhttps://js.driftt.com/core/assets/js/24.d1e2ba0d.chunk.js .https://driftt.com/..V.../.....?....k...4^.%w.[.z.Q..A..Eo.....A..Eo..... .....'.,.....O.....<.....(S....`.....L`V.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`..... .`.....Ma....0...`.....aN.....Qb..'....4bA0C..QbF..`....9qPMC..Qb..l.....AFWIC..Qb...S....BGieC..Qb.....BiFQC..Qb..".....FF9qC..Qbr.N@....IBDWC..Qb.V3a....O/ibC..Qb...5 ....SLDQC..Qb.....TxngC..Qb.&L.....UQjNC..QbR<.....ZkW+C..QbV..+....c4IMC..QbNbZ.....oxCZC..Qb.....peugC..QbF..)....qAzGC..Qb.5.....rGTNC..Qb..Y#....uqJV C..Qbn.M.....voa/C.(S.x.`.....4L`.....@Rc.....QbFd.....r.....S....M.b.....`.....Pd.....push.4bA0...a.....(S.....Ia....7.....Qe.....HTMLReactParser.....@.-....HP... ....9...https://js.driftt.com/c

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\791d5b9834f8c9fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	71840
Entropy (8bit):	5.5619848472115025
Encrypted:	false
SSDEEP:	768:vBucuITbfPY7k7Xj/ZVOJ41xUQP4M3/9fkSP4qSXbbVXdmsN8fpMZ+R/xjo:v8lTzY47TRD1uQ9VkO2XJYl8fpMZ+9u
MD5:	D105124ED00742D8874911B9025F478F
SHA1:	BB8CC9F7981C43011BE935D8648B91021CB1BD55
SHA-256:	395878CEC48E99BC6B47E86F69774143C910C95ED5B33266F5899E2057BC4860
SHA-512:	303247EBC7DC51E9A88028551D44575920C01ED7B58F0A48DCE8D294195E5B97FC0A3F93CC8918CB56AED04379C7E3E42C6A4DF29A06FA865AB9C25F819C7F F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\791d5b9834f8c9fd_0	
Preview:	0\r..m.....@...t.....EAEC76518B7579BCED0FD4B22986F51644212DF0A52460AFAE88C744CBDE21EF.....'.u.....O....h...".!s..... .....(S.....`.....=.L`.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push....`.....L`.....`.....Ma.....`.....-...a.....Qbz".,....+WaJC.. Qb.jZ...../V3TC..Qb...q....0ZCCC..Qb..{....13WSC..Qbb).....1VLmC..Qb.....2AHpC..Qb..^.....3yEJC..Qb.....4HYPC..Qb~Z'A....9OUNC..Qb.O.&....CxUuC..Qb.%..... .DwTnC..QbJ.....F5rfC..Qb6./.....FGAUC..Qb.}.o....HnWIC..Qb.vQ0....Jg5fC..Qb.:;.....JqiKC..Qb...C....LR82C..QbvP.....OEVoC..Qb.1.:....Q8hGC..Qb...Y....U3QCC.. Qb2..G....bacKC..Qb.,.....e7y7C..QbV6.Y....fQLHC..Qb...Q....gQstC..Qb...-....iJR/C..Qb&.-....icD7C..Qb.i.J....kOViC..Qbj..S....lUPPC..Qbb.Z.....pN2LC..Qb.....riKqC..Q b...V....s5AvC..Qb*f.:.....sna8C..Qb.Rz.....snleC..Qb...[....z5yOC..Qb._.6....z6NVC..QbB.E....zkdOC.(S.L.`P.....L`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8164647a8748d80a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.431024474421216
Encrypted:	false
SSDEEP:	6:mgYORz6+MEQT1FwSZQWK9+8C1zn1l7DK6t:9ZQTgqQWvhZ1/
MD5:	E57ADC13187B2E8C5C117FB1F67F9C13
SHA1:	E2B3063F082206A2E1AC92E6F5D3D30EEF6D3349
SHA-256:	DB2F02A7824191AC3459488EED1FC38E3ED64637B25A80B1A47237B4467D4ED0
SHA-512:	B1D0736C9DDB1C55D010AE6BF930D58E46993AF85BBCA54C0949A7D5467A244531DA9ABC3B6EBA50E138D63FC9ABA1B7A507E62CAFFC96BEE85FA112ACF41 AB2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...czL....._keyhttps://zix.com/themes/custom/zixappriver/js/main.js?v=1.x .https://zix.com/...../.....<$.....IGs.{.n..G...n.9...i.}.q..5..A..Eo....._.....A. .Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85eb2726a8e59d21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	58478
Entropy (8bit):	5.632581071623261
Encrypted:	false
SSDEEP:	768:Zxb4oRU/fUfLHfoxWjsXgVK6oVdY5Vupf2sGyuEUvbGom6/3BUybCk6k:klsfTWCVK6adP5GyuEsGG/BUybCkV
MD5:	9AB19334B859A4CF20FEE7C15F076B76
SHA1:	53BD73468BCE674958A5DD36200478BBADE5A98B
SHA-256:	2E86F3DCD070519B377BAF03D44C172B8F5667054D2568E35D24F199350CEC91
SHA-512:	90701C8D2546DFB0D4D4891D1CDC939EC6F03DCC982AE033801DCB14017BFF4D1ABC8F8C638F364AD00FD39AB427C0366191E6B5308E4D98CE51AEE7C0CB4 80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://js.driftt.com/core/assets/js/12.8c7dd5ee.chunk.js .https://driftt.com/.wC.../.....I.(a&...K....i.~.....,..f....A..Eo.....@.L.....A..Eo..... .....wC.../.....I.(a&...K....i.~.....,..f....A..Eo.....B.....'.zt....O....h....>.....(S.]...`n.....L`... ...Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push....`.....L`.....`.....Ma.....`.....a.....Qb..Dd....0B8EC..Qb.....0L1VC..Qb...q....37XjC..Qb...o....4Zd6C..Qb .....6rNQC..Qb>.. ....8dq5C..Qb.j{.....8lq6C..Qbf.....8s1RC..Qb..w.....9A2/C..Qb..{.....AqQoC..Qb.W.M....BCC6C..Qb...r....Bmr4C..Qb.....C7P9C..Qb.....CDfdC..QbR@. ....DboLC..Qb6..G....DdK4C..Qb.^.....FgEvC..Qb..{{....H/qhC..Qbr.P8....INLmC..Qbj.c.....JhUJC..Qb.y0?....Jn/HC..Qb...0....JstdC..Qb.n.....K0ZhC..Qb..o....KwHbC..Qbv.{:. ...LVcXC..QbR.^..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8896057fcbff1c19_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.677665983566275
Encrypted:	false
SSDEEP:	6:mf1YGLSmXZCH3Xi6KHSn/tad8xoCEwkP4cK6tWf1YGLSmXZCH3X0S0yad8xoCEwf:oVc3naI+8lsqVc3kdl8lvr71
MD5:	7B13A2F1DD32FE0014624A2F8B5C832A
SHA1:	FF32714FE793227F0CC6FA40E934FD01B37EE6CC
SHA-256:	89A42280DBE2E1647139D6A8FC5E74FC8070E2D0774167A05F7DE197AD4C5C9F
SHA-512:	F45C32F0352ADF0FE843448B349002DB998B012B4F774F43AF6076C4D96E2F1FF40BE612390D9B4771BE34A1EA79D6097EE98E47D7F24138B178E6D766B09A8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O.....Pj...._keyhttps://www.googletagmanager.com/gtag/js?id=UA-91357340-1 .https://zix.com/.Ad.../.....*3...,T..:...3._.LI.....H...A..Eo.....v3.....A..Eo .....0\r..m.....O.....Pj...._keyhttps://www.googletagmanager.com/gtag/js?id=UA-91357340-1 .https://zix.com/...../.....$.....*3...,T..:...3._.LI.....H...A..Eo..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\89a3ee021aa8fff9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240600
Entropy (8bit):	5.973810007308437
Encrypted:	false
SSDEEP:	3072:luUK2fJdSvgyuFPyRiJLj+3y2RBHRleWG4tHozDen/yYLwov:0ic2F6RiJ3iywbleclzS/DLwov
MD5:	73D4A7630C44F06693A0368100A5263B
SHA1:	16498A637B3681248C808B5E22BCE6A516061BB8
SHA-256:	1FB80CFFA7D253DD193CEB57CFE481673EDF47A2451D55C8FB382AD3E94E1C79
SHA-512:	F45596081FFFD30F5B425BB27EA0FB80B98133BF092543CD99EFEF75770B7FBE4AC68CEB83EE4364D86563CFF3A5E3AF53A53A09C872F8A31730F78F4C863BA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...>7}.....FA918A432EEF2261D87FE94CE2FCF83AE4603ECC0A852BA9522DDE30C4A51659.....'..n....OK.....|.....(....&..... .....".."..h.....(S.e...`~ .....L`T....(S.p.`.....L`.....0Rc.....O.`....I`....Da8.....Q.@.....module....Q.@^.}.....exports...Qc~.....document.(S.....5.a.....a.....a.....a..... .a.....Pc.....exportsa.....I.....@.-....0P....."...http://eriglobal.com/js/default.js..a.....D`....D`....D`.....`v...&...&....&..q.&...(S....&..`8M.....L`@.....Rc.....8..... M...Qb.pg.....c....Qb.....d.....Qb..`....e.....Qb.t'.....f.....Qb2.....h.....S...Qb.\N....j.....Qbf.....k....Qbn\.....m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d86142e4c1aaf72_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10490
Entropy (8bit):	5.945829330918518
Encrypted:	false
SSDEEP:	192:ASWl3yp2rzx21m1aUZcZZJT5Du1l6y/2yiUVV4M41XEHADVy48fxz4SdywaQr:89yp2Hx21m/Zcno6yRf4t10g4vz44ow
MD5:	CEB8239BF1D2B98C1CF34FF93F7772FD
SHA1:	99572B8B04E414894EBA84D654BEC931B6175214
SHA-256:	FD21CB2901BC55D44C66C2105C53C16647BDBC424AE12199D26F9CD31465AA5B
SHA-512:	6D44E7D94F6C1E445E5537D786F19B18F6D1F701AD5C5F2B1BC4932EA8C87B0F0DE7465C9870D77B99C087E7A691D6818AB42B7C089E3349344B3E18E2245EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...{6H....._keyhttps://js.driftt.com/core/assets/js/runtime~main.643a3a55.js .https://driftt.com/4tC.../.....3.|(.....n.B.HT`C..*$"...VTC.C.A..Eo..... ...A..Eo.....4tC.../.....3.|(.....n.B.HT`C..*$"...VTC.C.A..Eo.....'.....O....('..gq.....(S.4..`$.....L`.....(S.1..`.....L`<....h Rc0.....QbF.....e.... QfB\.F....checkDeferredModules..QbFd.....r.....Qb..F7....c.....Qb.....t.....M.. Qf.n.....__webpack_require__...Qb.`.....o...g$.....I `....Da.....*...(S.)..`.....(L`.....M...Qbb.....push.....Qe..)T....hasOwnProperty....Qb.....call..Qc./.....shift.....K`....D.Q.x.....*..&...*..&...*..&..&.|.&.(...i...B%.*..&...&. %.*....(...&...&.%.*..&..*..&.Y.....&..0...%.L.&..F.%..Qw.....&...B.....4&....&.(...&.(...&.(.. &.Z...."....&.%.*.$&.0..&%..&..B.....&.]..((..*..(..,&.X...&.\.0.....&.(..2&.(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\90e0fc941053c5e0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	138328
Entropy (8bit):	6.179515661204663
Encrypted:	false
SSDEEP:	3072:zPQ4nTny41AiXzpOPVahWf5qoecLA70KNDsATO8h3:T/yYBXI/5dE4+O8N
MD5:	2AAB3E88EF5890002CF33238D76C92FD
SHA1:	E8E549142AC76270BCAD75E0402D9E5D5786B6A9
SHA-256:	693A3B8523A4E8FCD28172621CEB5383676B71D6F751CFAA1201C0ADDA7B2709
SHA-512:	8449EF3DDDDA1CAAF65A181F995B739580DA7C57802FF941DD0683252D69FBF7C4F4074EB489D23D764DDC9A2B498A7345264655F29D5F8F1FE0770EDD28CA2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...T.....9134BD9779881D1408BFFC5C3B22B44E0674A996AE084254BB1B7398C6CFADEC.....'.B.....O-.....bG.....!..... .....4.....t.....L.....@.....(S...`.....LL`"....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.. ....L`.....`.....Ma....D...`.....<..a.....Qb.....7nmTC..Qb.....8SysC..Qb~.j....YjNLC..Qb...E....aWzzC..Qb...S....emlfC..Qb.R.....w/UTC.(S.<.`.....L`.....(S.t.`.....L`.....,Q.. ~.....__REACT_DEVTOOLS_GLOBAL_HOOK__....Qc.j.L....checkDCE..Rc....J.....QbF.....e...`.....Qc.=.....console...Qc.,.....error.....Kd .....*...a.....Dw0.....' .....s..G...&.(...s..:'.....&.(...&.Y.....%&....&...%.....&.(...&...&.Y.....(Rc.....`....Da....p.....d.....P...P.....@.-....HP.....9...https://js.driftt.com/core/assets/js/34.fe729 046.chunk.js.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b493ae1aa245169_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14313
Entropy (8bit):	5.680855330485396

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b493ae1aa245169_0	
Encrypted:	false
SSDEEP:	384:glE+Rf0vpNKhwsoZvmrNkvCvBcLAOjPcwuKxwlUg1esZWP8:g2VGSNjUUC08
MD5:	8434FFA91E4063538F7A9A442EEF6FCE
SHA1:	8B912DF27FB7D61A17BD59C9C82E67324289E8A7
SHA-256:	465E50734E8A8D6CADA68172963C18DDBD231ED594CCD854532F11F4432718EF
SHA-512:	040CD769F15371F482B81AB9A65444B16B68CAB05D7E14101B2AA3F436926BDF67AEC511D398A24C29F2F57B731EC6B553947BA6684E3A8564D3E0CE8D99C52
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...O..(...._keyhttps://js.driftt.com/core/assets/js/2.04b0c69b.chunk.js .https://driftt.com/:*T../.....r.....G.Uyr\x.L..k.i....G...X..$P..2..A..Eo.....F/`.....A ..Eo.....'..m....O....h6.....I.....4.....(S.....`.....L`^.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma..... .`.....aV.....Qb.'u.....+KbsC..Qb..z...../UYIC..QbV.....1GGFC..Qb.....3x/iC..QbJ5.8....58kBC..Qb..W.....908pC..Qb..Q.....GtSEC..Qb.O.....OyKiC..Qb2.....Sn8XC ..QbZ.....VpmRC..Qb^.M.....Yl0QC..QbfJ6.....f/zSC..Qb.4.....hSLTC..Qb.....j1wgC..Qb... ....kXeLC..Qbvy.....lE29C..Qb*.!.....nJ3uC..Qb.\.....nQD+C..Qb.@.....rTktC.. Qb~>.}....yEslC..Qb.@ .....z24sC.(S....`.....L`X.....RcL.....QbFd.....r.....Qb.`.....o.....Qb..F7....c.....S...Qb.,(.....l.....R....Qbv.47....d.....Qbv.....s.....QbRF .....f.....Qb..D (....h.....QbN.h,....v.....Qbv].....m

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9bea1099a402aeb8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.6068985836231215
Encrypted:	false
SSDEEP:	6:mLVYvI5sPXDxVISlAYnX0tH1T+E4fbK6t:kPsPXZORewEK
MD5:	1888C18D806984EDDC17F657C6E4298E
SHA1:	E46F867235F6B8EE8D4AFEB0D969AA8EFC2B51AD
SHA-256:	BA9BF2CCD588A6438288F41FC2B513A3D98F4542D266051003473AB8FF89B260
SHA-512:	0A63025943547BFB43D5C4BE09C0149F6AC8B8479F00157530D4519ADCAF23F765F66C5CADFD7F71BBED35EB1EEC25E863FA97E8687166297CD06718BDA9F39 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....W....._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/userNotifier.js .https://zixmail.net/...../.....Ti.....R.lu..}...).A.....A..Eo.....(.T.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9c58a5bd2d855331_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.895934002192763
Encrypted:	false
SSDEEP:	6:m4W9YZDtVcmWyAadJD8PSpKXzuYmMYFcZK6trMTrFBC2TSi3kW+oGuYmMYZ:+6Vx0eVMaKj1TtqBCkSCf+oGa
MD5:	CB50CF2E2E213ECCF15D84EFC30EBF60
SHA1:	C4B8053C0BB71F7CA05511DED5BD46662E66D535
SHA-256:	91F826B6B448394EF733166C90A772EF9C552250ED35DC7BDD1578D9B12B3656
SHA-512:	05F125FC329980D9B2B632D655FF3DE76E0E7C765F8768FD98AC1D98B17E6B466200C519FC299B80815C672991581906BF3AB8743F2AC666E26F872A3D973B08
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....j....._keyhttps://js.driftt.com/core/assets/js/25.5675afde.chunk.js .https://driftt.com/.@T../.....n..V..l%....5."..eQ...g..Z..C.X.A..Eo.....A..Eo..... .....@T.../.x...C2C2962F4479220E01CB960766EA055E6218399988A7D3785448C3BE8BB02AB1n..V..l%....5."..eQ...g..Z..C.X.A..Eo.....SL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9ff8bace99163776_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33298
Entropy (8bit):	6.136571408969595
Encrypted:	false
SSDEEP:	768:NQrOcDHKa/qvp/ZUEzmWlnZnK1c4l0uQ0gKZ4rL:NQrOaHKasRvlYNmuQ0sL
MD5:	D6337CB045A9C3CD6E167F2A2526A604
SHA1:	9FF0E8FA8C5716AD5C6BF616FF402CA792E50409
SHA-256:	243E99EA84ED4C6F7F39FD7256C5ADA32D63A00EFFF3B3D6FC3157A9DD940353
SHA-512:	1312059411 97B577E682DBAE46A7810C67F7F1C82848A8FEDE4F168F0EB9711D7A562F0BB97525DC918B3BB463E29BCD91EE661A44FFB0C73299DCE92ABBFF7 E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9ff8bace99163776_0	
Preview:	0\r..m.....R...i.R....._keyhttps://js.driftt.com/core/assets/js/27.899f51de.chunk.js .https://driftt.com/..V.../.....'.....wO.....7z.]Z./-..a.Rz.4.a.E..A..Eo.....d.....A..Eo.....'.M>....O....x...D.....(S....`.....tL`6.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push....`.....L`.....`..`....Ma....6...`.....d..a.....QbBu.....1I2JC..Qb~K.....97O6C..Qb..Y.....Gxm1C..QbB_^A....NCI6C..QbR[I.....SrLZC..Qb.P.....SwvNC..QbN2.....hNWdC..Qb..YZ....sXTYC..Qb..Q.....vwUFC..Qbn9.....xNFZC..Qb.CmZ....y0onC.(S...`.....8L`.....HRc .....M...Qc.!...._extends..QbFd.....r.....Qb..F7....c...c.....`.....Pd.....push.1I2J...a....j....(S.....Ia....k.....d.....@.....A...!..@.-....HP.....9...https://js.driftt.com/core/assets/js/27.899f51de.chunk.js...a.....D`....D`b...D`.....`....&...&..q.&.(S.....Iap...|...I....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a6864e076f152ec3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31910
Entropy (8bit):	5.744622095586981
Encrypted:	false
SSDEEP:	768:yTTda8tVngQPBayPFdx0S4QB6W+eZ5v3xfc2Xs1vqnFSBTPBS:yTxztVJ0CBrZ5/xflOqnFATPo
MD5:	90CA4EFE8E7E46D12E8119EA2F578903
SHA1:	30C708CFE3B828E956C3A8C98EA01787559D941A
SHA-256:	2D1DFEA45DFF4519DDC1A21631295987DD1A11A329FE90D4D7B67C45DE12C36E
SHA-512:	CD3C93D1EC40784D4876BF3CC494B5D6344BED6940EAE50F45F07BEB6ADCFE7271024AD3F71E0F0B50F88FE7ABC4E8406E06B2EC47B048A1C266AABB47BACF8C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...3..p...._keyhttps://js.driftt.com/core/assets/js/33.6dcbce8f.chunk.js .https://driftt.com/Z|C.../.....A.p....Q.]....DY...CJ&.fS-..]F..A..Eo.....|.....A..Eo.....Z|C.../..... .....A.p....Q.]....DY...CJ&.fS-..]F..A..Eo.....pI.....'..^....O.....z...9.....x...$.....(S...`.....TL`&.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....B...`.....D..a.....Qb..m.....EfWOC..QbB*.....aUJjC..Qb._.....aYSrC..Qb&>.....cyaTC..Qb..._....fRV1C..Qb..w.....qXcpC..Qb".....s+nuC.(S.....Pd.....push.EfWO...aG.....`..uM.....@.....@.....@.....@.....@.....@...".."..@.#.:..@.:.;..@.....d.....!.!..@..U....1.E.@.-....HP.....9...https://js.driftt.com/core/assets/js/33.6dcbce8f.chunk.js...a.....D`....D`$...D`.....`B...&...&.....D&.(S.P..`Z.... L`.....@Rc.....Qbv....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2f66da88d7b43b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	62137
Entropy (8bit):	5.923965296235672
Encrypted:	false
SSDEEP:	768:yt33fClzl2Knbf3MclDdcFzWsgxh8Kml8Kj/L7KLrWvzDLtgjiwYSRcLPujp:yt3vGJ2KjcIu/Y8Kml82D7KLyLZIsP8p
MD5:	51F0FA634133513BEBCA6DF836AEC655
SHA1:	11E66A0662332594C86013B351D5F2D72B58F2F0
SHA-256:	A2AA0A3B93C43FA4E7E8A2B5FD89F1C6DC71C7FEE6E1D7D80571C07C02EF0B72
SHA-512:	2996B02CBE6F84C03606EF2C9F126B475E188A35CC1AF10A39A5E313309A8ECBE44583DACEB803E263CC5A639BDB2E8B63F7AD31A512AACE621CDB5DBD7EE8AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,....._keyhttps://js.driftt.com/core/assets/js/main~970f9218.06709018.chunk.js .https://driftt.com/.~C.../..... .....R=$[.....s..g.,..1...[.....A..Eo.....E,.....A..Eo.....~C.../.....%.....R=$[.....s..g.,..1...[.....A..Eo.....:.....'.....O.....T.....(S....`^.....L`B.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.....`.....|..a:.....Qb...../7QAC..Qbr.....9ttKC..Qb.u .....K7i0C..Qb^.\.....La++C..Qb..JK....PCkZC..Qb"6C.....SFoaC..Qb.`.....SsZNC..Qbv.....TDUEC..Qb*~E.....WjfvC..Qb.q.....YA8zC..Qb2.....bYXQC..Qb.z.....qixEC..Qb..9V....vjChC..Qb.....y0ArC.(S.1..`.....L`X....8Rc.....Qb.....n.....QbFd.....r...a$.....`.....Pd.....push./7QA...a....d.....Qb^..&....pNMO..Qb.0.....DEfu..Qb*..{....I9xj..Qb~

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb0383b41217c93d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.4462818787611065
Encrypted:	false
SSDEEP:	6:muVYGLkHC7LEIN9gEHT1F0S9SSlOXlK6t:tqZvlE
MD5:	ABD2ADCE40C94DA2527FD17D388356A9
SHA1:	35C19B7A159622FE763B88D73922A54083382569
SHA-256:	D02264FECCE14E937D9EE618B3DDA59DA8DBE96004A5DEEA0E266480833B8B5D
SHA-512:	5817F13252550342F06AC6C768B898DC21B9CC3D6CDD8322B2576D42C7A04A4ADDF940AC21DFBAD6A6E91550BC555EFE97B3E8DA04AFEAC4CDACD4A296D3DE1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb0383b41217c93d_0	
Preview:	0\r..m.....X...H..-...._keyhttps://www.zix.com/libraries/bootstrap/dist/js/bootstrap.js?v=1.x .https://zix.com/...../.....u.....r.....J..KA.....URK.GC+c..8.A..Eo.....La<1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bd3855900f676b3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.411464856873204
Encrypted:	false
SSDEEP:	6:mSYGLkHGMQTqBntSTte07KPY4f1lDK6t:DMOqvkT8v1
MD5:	F484B67B36055CDA45509B51F214E0B1
SHA1:	89F726009E3A9C5F28D7642AC561EF00984ECD48
SHA-256:	826937FD578DFCE07058834D95AEEC4EF6A57D418A3D7DA78860C7DE23CA5761
SHA-512:	AB6712F7E38302B9904EC82E91A22EFB21F5272C98A1F6DA89CA85CCBCD3C80799C00523BD6DA0801807126F4ED55095501C0BAF8D72EE831552AB3847A7262
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F...x2....._keyhttps://www.zix.com/core/misc/drupal.js?v=8.9.10 .https://zix.com/...../.....=.....hX.`if/..F..fN.p.2.O..A..Eo.....F6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf80d895833efe33_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	325
Entropy (8bit):	5.847994338941401
Encrypted:	false
SSDEEP:	6:mlpzew4zl5lSUejlCqAbpK6tlQtDmlFdxwoSlCqAoL:x55lJqlCqejOimlFd+jlCq
MD5:	A5066FCAADD4B5513F050C2C693BC0FC
SHA1:	54EC419DAD07C78FD01358D1D9781B3692536A9D
SHA-256:	CA2373D7332D0F56718ACC0EA225FC766AEE0AE456E3D5B728322F8B411477A8
SHA-512:	600067A0F284FF02AC1B83F6ECDFC13E1F7929BBF0B3598FBE9E49672F3A76A972D41672E74630777B479347D64C5A4150C08AE70040AE47E63534A688065807
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=...<e....._keyhttp://eriglobal.com/js/default.js .http://eriglobal.com/...../.....p.....&..09..f.....S..CyZ|j.B'...A..Eo.....jTr.....A..Eo...../.0...FA918A432EEF2261D87FE94CE2FCF83AE4603ECC0A852BA9522DDE30C4A51659....&..09..f.....S..CyZ|j.B'...A..Eo.....MJ..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0e42b091147ff06_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	39433
Entropy (8bit):	6.022455949574092
Encrypted:	false
SSDEEP:	768:arsmJUzIDFbqH3c5+dxsS+o2eySA/tZ7yvz:exJAIDF9Sxr2e3A/t1yr
MD5:	87745051CF7D044A8337CAC736B92B11
SHA1:	E45E9837525C4780CBCA361E6E713BD90C613591
SHA-256:	CB40DC5AA8933514140A2F218D4906E77DADA405A93F2BD34B7D85CBD5F5029A
SHA-512:	41AB9D921CEFF5094FE19B1CCAB50BF390D6B5CAFCF0888A7D013671F9F5D2449446889CB4DA168985F80708FC5716FA1554130D4F41881486274908ED43878D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....._keyhttps://js.driftt.com/core/assets/js/main~493df0b3.1bfc4c5f.chunk.js .https://driftt.com/.}C.../.....s.....=.....%D..:.....6..A..Eo.....S.....A..Eo.....}C.../.....#.....s.....=.....%D..:.....6..A..Eo.....'..S....O.....E.....H.....X.....(S.-...`.....L`h.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma.....`.....ad.....QbNs0.....+/JeC`....C..Qbr..<....7oh4C..Qb"6$&....91+0C..Qb..k.....DFuOC..Qb.Lq[....GMUsC..Qb:,M.....LeJ0C..Qb.k.....LelFC..Qb..P.....LqZ+C..Qb.i.....OE2qC..Qb.k@.....QtlZC..Qb...0....SHZQC..Qb.z.....SWQ0C..Qb.r.....YvItC..Qb.-$.....efbEC..Qb.N.....ka07C..Qb.Lg.....mssFC..Qb"xC.....qSAjC..Qb..C[....r/xDC..Qb.....tXSlC..Qb.n.....vEWTC..Qb.....vTYTC..Qb.A8....xXFfC..Qb*l.....yKvLC`.....(S.h.`.....$L`.....8Rc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ca75a81802d989a1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.583180681704063
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ca75a81802d989a1_0	
SSDEEP:	6:moQVYvI5sPXDaATI6wsvSlSMXkSunODK6t:UsPXjHws+VXI6
MD5:	ABC3BAB427B1DF67112026CC62652E09
SHA1:	3020722E8CC07DF14EC779F78D64F4EA291898EE
SHA-256:	C2459B367AE61E23DF942E0E6DFDDF456B8E446311C8DE3CE583927A4E849370
SHA-512:	D20CE43C75593092EA981190FE7BEC8A1AA20A4DE63FBB7A1659924E8D82681D97F6316B94EBE6184580CD4B6F2E6BD5C465E3FE095033169EFD83290DBF843
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...qx.K...._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/default_registerview_validator.js .https://zixmail.net/S...../.....Bi.....?\rBKX\!.....U/4.-\V.(.$A 9.A..Eo.....1;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\deeb90394251543d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	478
Entropy (8bit):	5.605284816396683
Encrypted:	false
SSDEEP:	6:mUbEY02pzVMCovYFxSTKz6d4VxK6tWUbEY02pzVMCovYFHS4/yz6d4anK6t:pIqzVMCogdGIzIqzVMCoa5/yG7
MD5:	58BF51933E2415C7D5C15DA87AC892E1
SHA1:	2308CE2F4F870871FC822605113D27D874BD6A3C
SHA-256:	BEE832CE2FDA6E8A4A7CB9CC65863BD9CBE2C7CDA129523B77AABECEEE11ACD2
SHA-512:	BF634839A0ED647A7BAD2466ADB039A0E5C9E1F805599B121C65898965B775E414F38A0384B3967CEF53ADA62E10A42090E5097EC38758F6C914B7DBD32534CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....z1....._keyhttps://optanon.blob.core.windows.net/consent/c69ead4a-1411-40a0-a557-adb00027090d.js .https://zix.com/Y.h.../.....dw/O.g.g..h+.}...)_.. ..R{.BB..A..Eo.....`.....A..Eo.....0\r..m.....k....z1....._keyhttps://optanon.blob.core.windows.net/consent/c69ead4a-1411-40a0-a557-adb00027090d.js .https://z ix.com/.5..../.....Z$.....dw/O.g.g..h+.}...)_....R{.BB..A..Eo.....X,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\eadf69b2511119d6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.5747833638553566
Encrypted:	false
SSDEEP:	6:mHPYvI5sPXDlfLzIJlS+E4ptePH4chK6t:EsPXu5ZkL7
MD5:	67279C5947D7670801629D16770112D9
SHA1:	D7E1F8F53C4EEA1621982403C80040FEB4B11C3C
SHA-256:	83ADD5BF9B57B087A9B1F8DFE07F0105B02793B7620B301B395D24CD61EA4124
SHA-512:	878444096C66D90B70B29FF4273943A9B4F92574F2C8F87D5E3BCBA4ABD966D5EF65B6E1030A043EFECCA8959DDFE13A6B1A672B5C3EBF17F645CCC88667D5 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....'M....._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/emailfieldvalue.js .https://zixmail.net/...../.....Qi.....2...\..mgG.J.#T{..f...y.uv0Z;.A..Eo.....O._..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ed6f4c080ca8024e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.564880674846378
Encrypted:	false
SSDEEP:	6:mKVYvI5sPXD/u4SQlS/J/PegQC6hzrGZK6t:FPsPXTWweJeP5hzy
MD5:	C2B0CA7EC0A51BAC703E55CCEA28B2A5
SHA1:	4CC4C1CC7DA60E5F1CFD4C4338B7E9050ED121B1
SHA-256:	B3EE90845B796CF89E6BF69E438EE896A507DB47B1E14F08159CC24DC30465BB
SHA-512:	66712C2D39EF3F408871143565842E44D49A7DCB354F603988BD40283905902DCF6D98857389CF8561C53C7E159A3002555FB8301764D09FE1E3D63A1A230D65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://web1.zixmail.net/s/REL-5.11.17.280/scripts/jqueryui-custom/jquery-ui.js .https://zixmail.net/...../.....I.....%.\....r.h8...%a9G.WWW.....p..A.. Eo.....@#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\efc82e9adcf42c5c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	110880
Entropy (8bit):	6.0051304318995875
Encrypted:	false
SSDEEP:	1536:pw7PMUcRBnxtH48lZvchcY4mz5oO2n06mVUP4njV82t5kIM4Tiw9U64yzraI:pMMRrnxq8lZceY4m/35nx9tMk9SySI
MD5:	A6D9C27C7BC3AB592703AABAFA9599BC
SHA1:	B06C56E7BAFC55447D2C5F03D90D82F989CDD45E
SHA-256:	E588738C79A4BE07ECB08A7E437CD8E615BEACE687D26C49EC5B0AFB392858A2
SHA-512:	A3A3F541B9A98A8859A01DAA7E10DF3CF0F9031CB3263FAC39AB82F98B06F3CEB1DC35B69691B36996A238E1C2BE53E88E7582E594E89AD3614DDC251963AB0C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....7.i....C2C2962F4479220E01CB960766EA055E6218399988A7D3785448C3BE8BB02AB1.....'.....O%.....8.....@.....T...L.....(.....d.....|.....(S....`n.....L`F.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....2...`.....a>.....Qb2Z.....3y+jC..Qb.*.....6wvXC..Qb*.Tn....7fJ7C..Qb..Y.....Gxm1C..Qb..D....LwEIC..QbF.W.....My8UC..Qbj.VW....NJR1C..Qb.....ab+KC..Qb../....fL0fC..Qb"8T.....nedbC..Qb...+....o3t1C..Qb.{4.....pUpcC..Qb.pe.....tLIiC..Qb.CmZ....y0onC..Qb.....z8n0C.(S.$.`....]..K`....Dc.... .....(Rc.....1.`.....Pd.....push.3y+j...a.....@.-....HP.....9...https://js.driftt.com/core/assets/js/25.5675afde.chunk.js...a.....D`....D`N...D`.....`>...&...&....&.(S.H..`F.....L`.....8Rc.....M...Qb..F7....c...a.....q.`.....Pd.....push.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f2c5b710fbc9e04f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	61138
Entropy (8bit):	5.969670531706957
Encrypted:	false
SSDEEP:	768:VBEoGg6U6jUIoGS3NSnXwK1TLU9A5bdebQWGUu0mzWd2Rr9nN6kmwtxGwz34a/t6:DEfkYoZCwK1TLvbdbfom7rRRia1sEm
MD5:	AB05E3DDF02F973603CB278FAA8B8D9B
SHA1:	183D9043F805D105939CAD6BF5E54E34D218564B
SHA-256:	2D0E92013F21FA60EE86DF63437698A723516D5E15A95B345C813153B2308175
SHA-512:	FFA26AD2BFFC7C08DE07F7127136BA934A3C47598B3B65AB7535BC6B8F9CDF4D9D386DE67C2485451A2311A345C5D62BE492A3FBB1A6FEAA5167821F2BB672D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....y....._keyhttps://js.driftt.com/core/assets/js/20.ec5afb3b.chunk.js .https://driftt.com/..V.../....."u.....M&.B..Q....f./.v1|w,.q..A..Eo.....{.....A..Eo.....'.....O.....x.....\.....(S.M...`N.....L`~.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`.....`.....Ma....(...`.....av.....Qbf.@..../mDGC..Qb^^.f..../vf7C..Qb*1.....0xiiC..Qb...Z....3fZ3C..Qb&[}.....7NtSC..Qb.....7VeVC..Qbz..w....CswFC..Qb6b.....EskpC..Qb..`h....JG7QC..Qb.....M+uAC..Qb... ....N19uC..QbRy[#....PupTC..Qbf.k`....QkDhC..Qb*..H....R46iC..Qb.v.....VBlBC..Qb...*....W+sfC..Qb6q.7....XuDIC..Qbz.....Zg6EC..QbJ-Me....Zjh3C..Qb...<....Zv2+C..Qbn.Uf....ca4UC..Qb.....gf09C..QbZe.....hCUBC..Qb..A.....k93sC..Qb.%p.....oFTCC..Qbb.....oPI6C..Qb.E.....ovDpC..Qb.....p2OqC..Qb.o.-....utatC.(S.<.`2.....L`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f2d69cb8ea7d653f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	398
Entropy (8bit):	5.414227922873826
Encrypted:	false
SSDEEP:	12:I2IwvtlOc9Am6kF7D2Iwvn/m5tC9Am6k9:kIQtlDArc76IQ/maArE
MD5:	C268DEC3A2CFD28119728D555534A2E2
SHA1:	792D2FADEA210B4D5C63A5EF61E0522B8B445D40
SHA-256:	4A9AA4271132CDD9AB921F996AF339BB6EE1FEF34BFC5270EDCB6F051C66AD3B
SHA-512:	9FDD65C2FB2DD8A9432F1AFC25C88050C1E2F4A263FA59386C25E70DBEA1C47F34C59E8D9027C9CEBA9443BA898FD64BD5F54036F23CF8F0887696FAC565CAC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...9.s....._keyhttps://www.google-analytics.com/analytics.js .https://zix.com/B&s.../.....7.....o2.....CA2.&k_....tl.K2uLk...3.A..Eo.....,7u.....A..Eo.....0\r..m.....C...9.s....._keyhttps://www.google-analytics.com/analytics.js .https://zix.com/.&..../.....0%.....o2.....CA2.&k_....tl.K2uLk...3.A..Eo.....$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f39e117abfee7d27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f39e117abfee7d27_0	
Size (bytes):	329
Entropy (8bit):	5.907139782758711
Encrypted:	false
SSDEEP:	6:myCnYeSSIlJlSlqh3Kf49nazlhK6t7JVTBvUmwrZ3Kf49n:uRLITlWf49azl79DTBvc8f49
MD5:	A1671178836F1DE57174506E5185F3F9
SHA1:	E8D8E1FBA614BBC14BA130A7C4A27AC7591E0B45
SHA-256:	B0D15C9894D742E73EF6EB8C9DF0B9A28BE546E48EDD92C6A35E4FF847B3F038
SHA-512:	DEA5E39EBF626696CC9CC5ADEB25F140FFEAD8EF175F3902CD4E9843CB030622A9A3B44F3744A790D92183E2EE8B72836A3B8A141EB293B415913535B1ADA45 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A....._keyhttps://code.jquery.com/jquery-3.3.1.min.js .https://zix.com/.Ox.../.....j..-1:z....).....z....A..Eo.....UK.....A..Eo.....Ox.../. .w..D6247ADC89A02974E028021BCAB45C2A6A79E5753E94B8B9D7447CD6C1E81633.....j..-1:z....).....z....A..Eo.....PL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f4458942201558ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.8466747676785
Encrypted:	false
SSDEEP:	12:FRGVxq4VQePFgqEQN2ekFgqhH83XKmkLFgq:FAV7QelEQN5+KE
MD5:	AB872A961F03E6E86D1BE34F5E76CFCE
SHA1:	4DC39290C14F687C757C4F6A8441D1DA734FCE72
SHA-256:	9CF66E837ADAA27CDFC6E8BFA00182056999360D438FDD71846BA141B9CB9F59
SHA-512:	4E4B0F40729CBD72BB3E0D3FA5CA1947DD111AF64DEDF16BA6B2C6155905EABCCA972438B1F1F2B03A7787B59AC90129FF0A7551E05121010111B44B5F1757B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....t,....._keyhttps://js.driftt.com/core/assets/js/15.ba891359.chunk.js .https://driftt.com/.xC.../.....i.r.y.?.L.....F].....f%.....A..Eo.....uS?.....A..Eo..... .....xC.../.....i.r.y.?.L.....F].....f%.....A..Eo.....^.....xC.../.....EAEC76518B7579BCED0FD4B22986F51644212DF0A52460AFAE88C744CBDE21EF .i.r.y.?.L.....F].....f%.....A..Eo.....(..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f526fee988bc24e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	34594
Entropy (8bit):	5.676238220573257
Encrypted:	false
SSDEEP:	384:/q/9T2T2uAmkFa4lyxec2YHqZ9pyUk5OkTBCIO8fnK9z+U0wZnkvoUqtToqYBXXP:uVmZ419kYKj8TfYBXXeEfASLIrP2/MI
MD5:	0D98030E3EE07C1FEFA5BE66423DF454
SHA1:	F41E3C17CB8B962390C39AE3C13B72C44AB8AC94
SHA-256:	471102C3C3C5DC44A250F47839B29C69F115BAC11C806B5C7F4FB72D9B449FEC
SHA-512:	F2FBD83756533B3E94C0FFC643F5FB0CD7F74987CCF22F1D1D38E2D23A7DE06F69EFC3B2CDDEB997F9E1960168E90953F8C1D49D6A545752A1EB21E637EBB4 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...N....._keyhttps://js.driftt.com/core/assets/js/19.d206834e.chunk.js .https://driftt.com/R.V.../.....*..x...j....fb.A.T./.y.....M.0.A..Eo.....A..Eo.... .....'..E....O.....K.g/.....8.....(S.M...`N.....L`~.....Qc.....window....Q.P.PM.....webpackJsonp..Qbb.....push.....`.....L`..... .`.....Ma....&...`.....av.....QbR.....1b8iC..Qbv.l.....2uLeC..Qb..$.....6fy/C..Qb:.4y....6rzOC..Qb.*.....6wvXC..Qb.....7IKlC..Qb&.dx....8EprC..Qb..Dj....FJN1C..Qb...p ....MQZSC..Qb.2.;....P+wrC..Qb.J.....UAQ6C..Qb..x.....Vk0eC..Qb&.....ey6YC..Qb.C.-....fJpDC..Qb...b....fJrpC..Qb../....fL0fC..Qb...v....fpJsC..Qb.g.....fw6EC..Qb..... ..hhdZC..Qb.BiR....jITzC..QbB..!....kJB/C..Qb. L*....mZ4KC..Qb"8T.....nedbC..Qb&..8....nvPdC..Qb...+....o3t1C..Qb"..E....pwwTC..Qb.pe.....tLIiC..QbNM.X....uQkCC ..Qb.+8Z....xqp/C.(S.P.`Z.... L`.....@Rc.....Qb..F7...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f547e4ebb0310f07_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.619053147222318
Encrypted:	false
SSDEEP:	6:mwEYZDtLUACUSKTinnS2llSgslbgWGLpK6tWwEYZDtLUACUSKTinnFB9S7hlvslS:rLUAXSICl6OP9LUAXSIWB9slOOr
MD5:	C348E95542456FDBEDD62FA82C02189F
SHA1:	A226DAFC85BE15937625DB97F22C189B833B17F1
SHA-256:	4CE35BC2695F85E91ACD06560FA66D3A9D1F395A4A46EC8BAC368ACC3C7D57D6

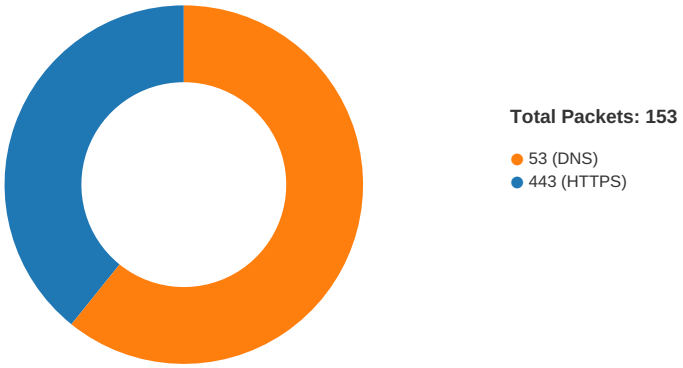
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f547e4ebb0310f07_0	
SHA-512:	F69AEE16B9B907E5CCA5B31230438819B77FB819CDBD05FD20FE242200418CE9068E7E588CD39BA66176CBDDFFECAB933FA7550D17D876F06B59C2ACCCC053A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...+.`....._keyhttps://js.driftt.com/include/1612410900000/65e63pi6mu5c.js .https://zix.com/4.w.../.....2.....P.....<..c~R3K...$...(.K.A..Eo.....C,.J.....A..Eo.....0\r..m.....Q...+.`....._keyhttps://js.driftt.com/include/1612410900000/65e63pi6mu5c.js .https://zix.com/.2.../.....%.....2.....P.....<..c~R3K...$...(.K.A..Eo.....@.....A..Eo.....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:50:02.108176947 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.109451056 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.189699888 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.271961927 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.271996021 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.272145033 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.272181034 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.274463892 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.274612904 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.352611065 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.352754116 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.353581905 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.438527107 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.439091921 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441721916 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441741943 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441752911 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441770077 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441786051 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441840887 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.441854000 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.441881895 CET	49727	443	192.168.2.6	63.71.15.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:50:02.482084990 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.516710043 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.519889116 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.519937992 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.519972086 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:02.520040989 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:02.561556101 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:03.872966051 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:03.874582052 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:03.876184940 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.035819054 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.036712885 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.037195921 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.037266970 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.037404060 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.037833929 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.038595915 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.038638115 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.039414883 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.039499998 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.040085077 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.040426016 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.040505886 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.202203035 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.247844934 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.247874975 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.247891903 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.247910976 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.247967005 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.248008013 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.342706919 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.344361067 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.344775915 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.345442057 CET	49741	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.345915079 CET	49742	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.346303940 CET	49743	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.506700039 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.507518053 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.507534027 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.508253098 CET	443	49741	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.508352995 CET	49741	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.508619070 CET	49741	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.509995937 CET	443	49742	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.510113955 CET	49742	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.510138035 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.510159016 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.510168076 CET	443	49727	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.510349989 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.510370970 CET	49742	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.510477066 CET	443	49743	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.510549068 CET	49743	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.510807037 CET	49743	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.512052059 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512073040 CET	443	49728	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512147903 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512151957 CET	49728	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.512171984 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512187958 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512219906 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512232065 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.512237072 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.512269020 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.515036106 CET	49727	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.518830061 CET	49728	443	192.168.2.6	63.71.15.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:50:04.552208900 CET	49726	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.671441078 CET	443	49741	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.671617985 CET	443	49741	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.671685934 CET	49741	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.672724962 CET	49741	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.673255920 CET	49741	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.675506115 CET	443	49742	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.675873995 CET	443	49742	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.676004887 CET	49742	443	192.168.2.6	63.71.15.50
Feb 3, 2021 19:50:04.676479101 CET	443	49743	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.676546097 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.676567078 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.676577091 CET	443	49726	63.71.15.50	192.168.2.6
Feb 3, 2021 19:50:04.676634073 CET	49726	443	192.168.2.6	63.71.15.50

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:49:54.699623108 CET	58384	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:49:54.747742891 CET	53	58384	8.8.8.8	192.168.2.6
Feb 3, 2021 19:49:55.936826944 CET	60261	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:49:55.985492945 CET	53	60261	8.8.8.8	192.168.2.6
Feb 3, 2021 19:49:57.235635996 CET	56061	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:49:57.281398058 CET	53	56061	8.8.8.8	192.168.2.6
Feb 3, 2021 19:49:58.406011105 CET	58336	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:49:58.454076052 CET	53	58336	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:00.185971022 CET	53781	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:00.233779907 CET	53	53781	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:01.940922022 CET	55299	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:01.943389893 CET	63745	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:01.947024107 CET	50055	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:01.947058916 CET	61374	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:02.007695913 CET	53	55299	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.007733107 CET	53	63745	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.009458065 CET	53	61374	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.106688976 CET	53	50055	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.535902023 CET	50339	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:02.605318069 CET	53	50339	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.631964922 CET	63307	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:02.638706923 CET	49694	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:02.668205023 CET	54982	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:02.692080975 CET	53	63307	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.702984095 CET	53	49694	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:02.715493917 CET	53	54982	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:03.420015097 CET	63718	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:03.487312078 CET	53	63718	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:03.776112080 CET	62116	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:03.802920103 CET	63816	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:03.833142042 CET	53	62116	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:03.852627993 CET	53	63816	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:05.165606976 CET	55014	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:05.220740080 CET	53	55014	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:06.205490112 CET	62208	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:06.267564058 CET	53	62208	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:06.316359043 CET	57574	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:06.367791891 CET	53	57574	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:07.045598984 CET	53799	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:07.099929094 CET	53	53799	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:07.598810911 CET	54683	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:07.649247885 CET	53	54683	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:08.843664885 CET	59329	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:08.889528990 CET	53	59329	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:09.970460892 CET	58177	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:10.016168118 CET	53	58177	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:50:10.477807999 CET	50700	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:10.544744015 CET	53	50700	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:11.247610092 CET	54069	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:11.324091911 CET	53	54069	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:16.205708027 CET	57017	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:16.266526937 CET	53	57017	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:16.638432026 CET	56327	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:16.703360081 CET	53	56327	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:18.633070946 CET	50243	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:18.698281050 CET	53	50243	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:19.772439003 CET	62055	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:19.774458885 CET	61249	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:19.775248051 CET	65252	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:19.820792913 CET	53	65252	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:19.822040081 CET	53	62055	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:19.830195904 CET	53	61249	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:20.013566971 CET	64367	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:20.072621107 CET	53	64367	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:20.116558075 CET	55066	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:20.133657932 CET	60211	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:20.165199041 CET	53	55066	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:20.187668085 CET	53	60211	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:22.179198027 CET	56570	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:22.240926981 CET	53	56570	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:22.472179890 CET	58454	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:22.648299932 CET	53	58454	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:23.129051924 CET	55180	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:23.184257984 CET	53	55180	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:25.893207073 CET	58721	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:25.917154074 CET	57691	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:25.949224949 CET	53	58721	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:25.966310978 CET	53	57691	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:31.741939068 CET	52943	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:31.744103909 CET	59489	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:31.799607992 CET	53	59489	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:31.804327011 CET	53	52943	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:32.382376909 CET	64022	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:32.438110113 CET	53	64022	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:32.480916977 CET	60023	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:32.535356998 CET	53	60023	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.074424982 CET	57193	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.130074978 CET	50248	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.131686926 CET	64413	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.132760048 CET	60429	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.133261919 CET	53	57193	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.180282116 CET	53	60429	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.188421965 CET	53	50248	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.198664904 CET	53	64413	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.596237898 CET	60345	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.617520094 CET	58730	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.663846016 CET	53	60345	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.663964033 CET	53830	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:34.666527987 CET	53	58730	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:34.732547998 CET	53	53830	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:35.330271006 CET	57226	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:35.395426989 CET	53	57226	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:35.582616091 CET	57880	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:35.584778070 CET	60850	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:35.586076021 CET	53187	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:35.641608953 CET	53	57880	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:35.648637056 CET	53	60850	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:35.649761915 CET	53	53187	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:36.410984039 CET	53190	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:36.461577892 CET	443	53190	108.177.15.156	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:50:36.461612940 CET	443	53190	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:36.503109932 CET	55830	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:36.506987095 CET	53190	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:36.564663887 CET	53	55830	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:36.568093061 CET	443	53190	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:36.570764065 CET	53190	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:36.571489096 CET	53190	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:36.621285915 CET	443	53190	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:36.621309996 CET	443	53190	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:36.627357960 CET	53190	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:37.997457981 CET	55145	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:38.043258905 CET	64091	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:38.057374954 CET	53	55145	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:38.100465059 CET	53	64091	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:38.379093885 CET	55728	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:38.414048910 CET	55694	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:38.435370922 CET	53	55728	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:38.472757101 CET	53	55694	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:39.517601967 CET	53926	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:39.578948975 CET	53	53926	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:39.884619951 CET	65531	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:39.947247028 CET	53	65531	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:40.150825977 CET	65437	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:40.177107096 CET	54590	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:40.212991953 CET	53	65437	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:40.237880945 CET	53	54590	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:40.584079027 CET	51318	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:40.632635117 CET	60888	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:40.645102024 CET	53	51318	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:40.689199924 CET	53	60888	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:41.279961109 CET	58474	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:41.304532051 CET	64575	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:41.327984095 CET	59092	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:41.336610079 CET	53	58474	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:41.358854055 CET	53	64575	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:41.387414932 CET	53	59092	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:41.877486944 CET	57483	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:41.934246063 CET	53	57483	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:42.942686081 CET	49809	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:43.000531912 CET	53	49809	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:43.999293089 CET	52814	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:44.173073053 CET	53	52814	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:44.377978086 CET	51069	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:44.423549891 CET	53	51069	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:45.276547909 CET	56526	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:45.335233927 CET	53	56526	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:46.384974003 CET	50512	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:46.430808067 CET	53	50512	8.8.8.8	192.168.2.6
Feb 3, 2021 19:50:51.573230028 CET	53190	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:51.648181915 CET	443	53190	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.523418903 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:53.573859930 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.574618101 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:53.574851990 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:53.574950933 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:53.625005007 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.625174046 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.625317097 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.625335932 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.625446081 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:50:53.625812054 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:53.629475117 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:50:56.460716963 CET	51679	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:56.516396046 CET	53	51679	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2021 19:50:59.747817993 CET	56071	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:50:59.812093019 CET	53	56071	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:00.796319008 CET	57035	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:00.842827082 CET	53	57035	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:08.589785099 CET	50522	443	192.168.2.6	108.177.15.156
Feb 3, 2021 19:51:08.664287090 CET	443	50522	108.177.15.156	192.168.2.6
Feb 3, 2021 19:51:14.148175001 CET	54122	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:14.205070972 CET	53	54122	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:20.034070015 CET	56759	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:20.088274002 CET	53	56759	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:20.602884054 CET	59220	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:20.657017946 CET	53	59220	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:21.172894001 CET	62211	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:21.235032082 CET	53	62211	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:21.643351078 CET	62033	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:21.697597980 CET	53	62033	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:22.112834930 CET	61244	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:22.170512915 CET	53696	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:22.171951056 CET	53	61244	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:22.226506948 CET	53	53696	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:22.633507013 CET	50733	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:22.697515011 CET	53	50733	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:23.166817904 CET	55770	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:23.225944042 CET	53	55770	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:23.782371998 CET	54525	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:23.844147921 CET	53	54525	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:24.747670889 CET	61760	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:24.801969051 CET	53	61760	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:25.310571909 CET	63822	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:25.369438887 CET	53	63822	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:30.147294998 CET	50957	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:30.206026077 CET	53	50957	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:30.230771065 CET	59666	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:30.291400909 CET	53	59666	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:30.397689104 CET	52223	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:30.453263044 CET	53	52223	8.8.8.8	192.168.2.6
Feb 3, 2021 19:51:30.579682112 CET	60136	53	192.168.2.6	8.8.8.8
Feb 3, 2021 19:51:30.642254114 CET	53	60136	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 3, 2021 19:50:01.947024107 CET	192.168.2.6	8.8.8.8	0x70d2	Standard query (0)	web1.zixmail.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:03.420015097 CET	192.168.2.6	8.8.8.8	0x31fe	Standard query (0)	ocsp.affirmtrust.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:07.045598984 CET	192.168.2.6	8.8.8.8	0xb79	Standard query (0)	web1.zixmail.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:10.477807999 CET	192.168.2.6	8.8.8.8	0xcb51	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:11.247610092 CET	192.168.2.6	8.8.8.8	0xed66	Standard query (0)	4eri.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:16.205708027 CET	192.168.2.6	8.8.8.8	0x496	Standard query (0)	eriglobal.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.772439003 CET	192.168.2.6	8.8.8.8	0xe82a	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.774458885 CET	192.168.2.6	8.8.8.8	0x22be	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.775248051 CET	192.168.2.6	8.8.8.8	0x5cc3	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:20.013566971 CET	192.168.2.6	8.8.8.8	0xccd	Standard query (0)	www.webdesignerexpress.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:20.116558075 CET	192.168.2.6	8.8.8.8	0x2f10	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:22.179198027 CET	192.168.2.6	8.8.8.8	0xb10	Standard query (0)	eriglobal.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 3, 2021 19:50:22.472179890 CET	192.168.2.6	8.8.8.8	0xa52c	Standard query (0)	www.zix.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:23.129051924 CET	192.168.2.6	8.8.8.8	0x85c8	Standard query (0)	ocsp.entrust.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.893207073 CET	192.168.2.6	8.8.8.8	0xe7a5	Standard query (0)	www.bugherd.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.917154074 CET	192.168.2.6	8.8.8.8	0x3ec6	Standard query (0)	optanon.blob.core.windows.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:31.744103909 CET	192.168.2.6	8.8.8.8	0x95d7	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:32.382376909 CET	192.168.2.6	8.8.8.8	0xe087	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.074424982 CET	192.168.2.6	8.8.8.8	0x4e75	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.130074978 CET	192.168.2.6	8.8.8.8	0x4118	Standard query (0)	js.driftt.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.131686926 CET	192.168.2.6	8.8.8.8	0x78e	Standard query (0)	tag.demandbase.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.132760048 CET	192.168.2.6	8.8.8.8	0xbbac	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.596237898 CET	192.168.2.6	8.8.8.8	0x349f	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.617520094 CET	192.168.2.6	8.8.8.8	0x33dd	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.330271006 CET	192.168.2.6	8.8.8.8	0x9f8f	Standard query (0)	js.driftqa.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.582616091 CET	192.168.2.6	8.8.8.8	0x6fcc	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.584778070 CET	192.168.2.6	8.8.8.8	0xa096	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.586076021 CET	192.168.2.6	8.8.8.8	0x9e50	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:36.503109932 CET	192.168.2.6	8.8.8.8	0x742f	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:37.997457981 CET	192.168.2.6	8.8.8.8	0x66d9	Standard query (0)	conversation.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.043258905 CET	192.168.2.6	8.8.8.8	0x55c6	Standard query (0)	customer.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.379093885 CET	192.168.2.6	8.8.8.8	0x88bc	Standard query (0)	metrics.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.414048910 CET	192.168.2.6	8.8.8.8	0xeb73	Standard query (0)	targeting.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.517601967 CET	192.168.2.6	8.8.8.8	0xf21e	Standard query (0)	www.zix.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.884619951 CET	192.168.2.6	8.8.8.8	0x1dd1	Standard query (0)	embeds.driftcdn.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.150825977 CET	192.168.2.6	8.8.8.8	0x1665	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.177107096 CET	192.168.2.6	8.8.8.8	0x1219	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.584079027 CET	192.168.2.6	8.8.8.8	0xe231	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.632635117 CET	192.168.2.6	8.8.8.8	0x3e74	Standard query (0)	bootstrap.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.279961109 CET	192.168.2.6	8.8.8.8	0xa62c	Standard query (0)	115079-29.chat.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.304532051 CET	192.168.2.6	8.8.8.8	0xbfad	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.327984095 CET	192.168.2.6	8.8.8.8	0xf5e3	Standard query (0)	event.api.drift.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.877486944 CET	192.168.2.6	8.8.8.8	0xec6f	Standard query (0)	www.zixcorp.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:42.942686081 CET	192.168.2.6	8.8.8.8	0x48c3	Standard query (0)	ocsp.affirmtrust.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:43.999293089 CET	192.168.2.6	8.8.8.8	0xc569	Standard query (0)	zix.com	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:56.460716963 CET	192.168.2.6	8.8.8.8	0x8674	Standard query (0)	zix.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:02.106688976 CET	8.8.8.8	192.168.2.6	0x70d2	No error (0)	web1.zixmail.net		63.71.15.50	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:03.487312078 CET	8.8.8.8	192.168.2.6	0x31fe	No error (0)	ocsp.affirmtrust.com	ocsp.entrust.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:07.099929094 CET	8.8.8.8	192.168.2.6	0xb79	No error (0)	web1.zixmail.net		63.71.15.50	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:10.544744015 CET	8.8.8.8	192.168.2.6	0xcb51	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:10.544744015 CET	8.8.8.8	192.168.2.6	0xcb51	No error (0)	googlehosted.l.googleusercontent.com		172.217.20.225	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:11.324091911 CET	8.8.8.8	192.168.2.6	0xed66	No error (0)	4eri.com		184.168.131.241	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:16.266526937 CET	8.8.8.8	192.168.2.6	0x496	No error (0)	eriglobal.com		68.233.236.236	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.820792913 CET	8.8.8.8	192.168.2.6	0x5cc3	No error (0)	twitter.com		104.244.42.129	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.820792913 CET	8.8.8.8	192.168.2.6	0x5cc3	No error (0)	twitter.com		104.244.42.193	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.822040081 CET	8.8.8.8	192.168.2.6	0xe82a	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:19.822040081 CET	8.8.8.8	192.168.2.6	0xe82a	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:19.830195904 CET	8.8.8.8	192.168.2.6	0x22be	No error (0)	www.instagram.com	z-p42-instagram.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:19.830195904 CET	8.8.8.8	192.168.2.6	0x22be	No error (0)	z-p42-instagram.c10r.facebook.com		185.60.216.174	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:20.072621107 CET	8.8.8.8	192.168.2.6	0xccd	No error (0)	www.webdesignerexpress.com		172.67.138.15	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:20.072621107 CET	8.8.8.8	192.168.2.6	0xccd	No error (0)	www.webdesignerexpress.com		104.21.48.217	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:20.165199041 CET	8.8.8.8	192.168.2.6	0x2f10	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:22.240926981 CET	8.8.8.8	192.168.2.6	0xb10	No error (0)	eriglobal.com		68.233.236.236	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:22.648299932 CET	8.8.8.8	192.168.2.6	0xa52c	No error (0)	www.zix.com		199.30.234.249	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:23.184257984 CET	8.8.8.8	192.168.2.6	0x85c8	No error (0)	ocsp.entrust.net	ocsp.entrust.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com	www.bugherd.com.herokudns.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		3.213.190.117	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		34.205.198.58	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		54.235.211.105	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		3.225.89.236	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		52.1.26.21	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		3.226.231.47	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		52.2.242.115	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.949224949 CET	8.8.8.8	192.168.2.6	0xe7a5	No error (0)	www.bugherd.com.herokudns.com		52.55.225.227	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:25.966310978 CET	8.8.8.8	192.168.2.6	0x3ec6	No error (0)	optanon.blob.core.windows.net	blob.db3prdstr11a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:25.966310978 CET	8.8.8.8	192.168.2.6	0x3ec6	No error (0)	blob.db3prdstr11a.store.core.windows.net		52.239.137.4	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:31.799607992 CET	8.8.8.8	192.168.2.6	0x95d7	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:32.438110113 CET	8.8.8.8	192.168.2.6	0xe087	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.133261919 CET	8.8.8.8	192.168.2.6	0x4e75	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.180282116 CET	8.8.8.8	192.168.2.6	0xbbac	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.188421965 CET	8.8.8.8	192.168.2.6	0x4118	No error (0)	js.driftt.com	dl7g9llrghqi1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.188421965 CET	8.8.8.8	192.168.2.6	0x4118	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.2.71	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.188421965 CET	8.8.8.8	192.168.2.6	0x4118	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.2.32	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.188421965 CET	8.8.8.8	192.168.2.6	0x4118	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.2.118	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.188421965 CET	8.8.8.8	192.168.2.6	0x4118	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.2.99	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.198664904 CET	8.8.8.8	192.168.2.6	0x78e	No error (0)	tag.demandbase.com		143.204.2.74	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.198664904 CET	8.8.8.8	192.168.2.6	0x78e	No error (0)	tag.demandbase.com		143.204.2.85	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.198664904 CET	8.8.8.8	192.168.2.6	0x78e	No error (0)	tag.demandbase.com		143.204.2.82	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.198664904 CET	8.8.8.8	192.168.2.6	0x78e	No error (0)	tag.demandbase.com		143.204.2.94	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.663846016 CET	8.8.8.8	192.168.2.6	0x349f	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.663846016 CET	8.8.8.8	192.168.2.6	0x349f	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.663846016 CET	8.8.8.8	192.168.2.6	0x349f	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.663846016 CET	8.8.8.8	192.168.2.6	0x349f	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.663846016 CET	8.8.8.8	192.168.2.6	0x349f	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:34.666527987 CET	8.8.8.8	192.168.2.6	0x33dd	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.666527987 CET	8.8.8.8	192.168.2.6	0x33dd	No error (0)	mix.linkedin.com	pop-tln1-alpha.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:34.666527987 CET	8.8.8.8	192.168.2.6	0x33dd	No error (0)	pop-tln1-alpha.mix.linkedin.com		185.63.144.5	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.395426989 CET	8.8.8.8	192.168.2.6	0x9f8f	No error (0)	js.driftqa.com		3.229.202.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:35.395426989 CET	8.8.8.8	192.168.2.6	0x9f8f	No error (0)	js.driftqa.com		54.197.143.221	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.641608953 CET	8.8.8.8	192.168.2.6	0x6fcc	No error (0)	match.prod.bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.641608953 CET	8.8.8.8	192.168.2.6	0x6fcc	No error (0)	match.prod.bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.641608953 CET	8.8.8.8	192.168.2.6	0x6fcc	No error (0)	match.prod.bidr.io		52.215.8.160	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.641608953 CET	8.8.8.8	192.168.2.6	0x6fcc	No error (0)	match.prod.bidr.io		54.228.192.197	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.641608953 CET	8.8.8.8	192.168.2.6	0x6fcc	No error (0)	match.prod.bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.641608953 CET	8.8.8.8	192.168.2.6	0x6fcc	No error (0)	match.prod.bidr.io		52.214.70.9	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.648637056 CET	8.8.8.8	192.168.2.6	0xa096	No error (0)	id.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.649761915 CET	8.8.8.8	192.168.2.6	0x9e50	No error (0)	api.company-target.com		99.86.167.33	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.649761915 CET	8.8.8.8	192.168.2.6	0x9e50	No error (0)	api.company-target.com		99.86.167.25	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.649761915 CET	8.8.8.8	192.168.2.6	0x9e50	No error (0)	api.company-target.com		99.86.167.117	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:35.649761915 CET	8.8.8.8	192.168.2.6	0x9e50	No error (0)	api.company-target.com		99.86.167.119	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:36.564663887 CET	8.8.8.8	192.168.2.6	0x742f	No error (0)	segments.company-target.com		99.86.167.90	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:36.564663887 CET	8.8.8.8	192.168.2.6	0x742f	No error (0)	segments.company-target.com		99.86.167.121	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:36.564663887 CET	8.8.8.8	192.168.2.6	0x742f	No error (0)	segments.company-target.com		99.86.167.76	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:36.564663887 CET	8.8.8.8	192.168.2.6	0x742f	No error (0)	segments.company-target.com		99.86.167.41	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.057374954 CET	8.8.8.8	192.168.2.6	0x66d9	No error (0)	conversation.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:38.057374954 CET	8.8.8.8	192.168.2.6	0x66d9	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:38.057374954 CET	8.8.8.8	192.168.2.6	0x66d9	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.057374954 CET	8.8.8.8	192.168.2.6	0x66d9	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.057374954 CET	8.8.8.8	192.168.2.6	0x66d9	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:38.057374954 CET	8.8.8.8	192.168.2.6	0x66d9	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.100465059 CET	8.8.8.8	192.168.2.6	0x55c6	No error (0)	customer.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:38.100465059 CET	8.8.8.8	192.168.2.6	0x55c6	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.100465059 CET	8.8.8.8	192.168.2.6	0x55c6	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.100465059 CET	8.8.8.8	192.168.2.6	0x55c6	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.100465059 CET	8.8.8.8	192.168.2.6	0x55c6	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.435370922 CET	8.8.8.8	192.168.2.6	0x88bc	No error (0)	metrics.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:38.435370922 CET	8.8.8.8	192.168.2.6	0x88bc	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.435370922 CET	8.8.8.8	192.168.2.6	0x88bc	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.435370922 CET	8.8.8.8	192.168.2.6	0x88bc	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.435370922 CET	8.8.8.8	192.168.2.6	0x88bc	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:38.472757101 CET	8.8.8.8	192.168.2.6	0xeb73	No error (0)	targeting.api.drift.com		100.24.186.63	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:38.472757101 CET	8.8.8.8	192.168.2.6	0xeb73	No error (0)	targeting.api.drift.com		34.204.215.213	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.578948975 CET	8.8.8.8	192.168.2.6	0xf21e	No error (0)	www.zix.com		199.30.234.249	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.947247028 CET	8.8.8.8	192.168.2.6	0x1dd1	No error (0)	embeds.driftcdn.com		13.226.169.56	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.947247028 CET	8.8.8.8	192.168.2.6	0x1dd1	No error (0)	embeds.driftcdn.com		13.226.169.125	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.947247028 CET	8.8.8.8	192.168.2.6	0x1dd1	No error (0)	embeds.driftcdn.com		13.226.169.31	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:39.947247028 CET	8.8.8.8	192.168.2.6	0x1dd1	No error (0)	embeds.driftcdn.com		13.226.169.91	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.212991953 CET	8.8.8.8	192.168.2.6	0x1665	No error (0)	match.prod.bidr.io		52.215.8.160	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.212991953 CET	8.8.8.8	192.168.2.6	0x1665	No error (0)	match.prod.bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.212991953 CET	8.8.8.8	192.168.2.6	0x1665	No error (0)	match.prod.bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.212991953 CET	8.8.8.8	192.168.2.6	0x1665	No error (0)	match.prod.bidr.io		54.228.192.197	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.212991953 CET	8.8.8.8	192.168.2.6	0x1665	No error (0)	match.prod.bidr.io		52.214.70.9	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.212991953 CET	8.8.8.8	192.168.2.6	0x1665	No error (0)	match.prod.bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.237880945 CET	8.8.8.8	192.168.2.6	0x1219	No error (0)	id.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.645102024 CET	8.8.8.8	192.168.2.6	0xe231	No error (0)	segments.company-target.com		99.86.167.41	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.645102024 CET	8.8.8.8	192.168.2.6	0xe231	No error (0)	segments.company-target.com		99.86.167.121	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.645102024 CET	8.8.8.8	192.168.2.6	0xe231	No error (0)	segments.company-target.com		99.86.167.76	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.645102024 CET	8.8.8.8	192.168.2.6	0xe231	No error (0)	segments.company-target.com		99.86.167.90	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.689199924 CET	8.8.8.8	192.168.2.6	0x3e74	No error (0)	bootstrap.api.drift.com		18.215.11.20	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:40.689199924 CET	8.8.8.8	192.168.2.6	0x3e74	No error (0)	bootstrap.api.drift.com		52.22.71.46	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	115079-29.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.198.218.148	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		35.168.188.71	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.218.95.178	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.73.109.12	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		174.129.151.215	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.203.160.252	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.224.160.94	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.336610079 CET	8.8.8.8	192.168.2.6	0xa62c	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		23.23.212.255	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.358854055 CET	8.8.8.8	192.168.2.6	0xbfad	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:41.358854055 CET	8.8.8.8	192.168.2.6	0xbfad	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.358854055 CET	8.8.8.8	192.168.2.6	0xbfad	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.358854055 CET	8.8.8.8	192.168.2.6	0xbfad	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.358854055 CET	8.8.8.8	192.168.2.6	0xbfad	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.387414932 CET	8.8.8.8	192.168.2.6	0xf5e3	No error (0)	event.api.drift.com	alb-event-1454785217.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:41.387414932 CET	8.8.8.8	192.168.2.6	0xf5e3	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		18.205.49.143	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.387414932 CET	8.8.8.8	192.168.2.6	0xf5e3	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		18.204.181.250	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:41.934246063 CET	8.8.8.8	192.168.2.6	0xec6f	No error (0)	www.zixcorp.com		199.30.234.249	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 3, 2021 19:50:43.000531912 CET	8.8.8.8	192.168.2.6	0x48c3	No error (0)	ocsp.affirmtrust.com	ocsp.entrust.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:44.173073053 CET	8.8.8.8	192.168.2.6	0xc569	No error (0)	zix.com		199.30.234.249	A (IP address)	IN (0x0001)
Feb 3, 2021 19:50:45.335233927 CET	8.8.8.8	192.168.2.6	0x389	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 3, 2021 19:50:56.516396046 CET	8.8.8.8	192.168.2.6	0x8674	No error (0)	zix.com		199.30.234.249	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 4eri.com
- eriglobal.com
- www.zixcorp.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49763	184.168.131.241	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:14.532562017 CET	2147	OUT	GET / HTTP/1.1 Host: 4eri.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Feb 3, 2021 19:50:14.750396013 CET	2147	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Wed, 03 Feb 2021 18:50:14 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://eriglobal.com Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49771	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:16.442796946 CET	2148	OUT	GET / HTTP/1.1 Host: eriglobal.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:16.808243990 CET	2151	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:14 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; path=/; HttpOnly Set-Cookie: session=8b6bfc69995572d35be50026df1c0741; path=/ Set-Cookie: lang=english; expires=Thu, 03-Feb-2022 18:50:14 GMT; Max-Age=31536000; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=20, max=300 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 61 36 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 0a 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 66 62 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 2f 66 62 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 0a 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 3c 62 61 73 65 0a 68 72 65 66 3d 22 2f 2f 65 72 69 67 6c 6f 62 61 6c 2e 63 6f 6d 2f 22 20 2f 3e 3c 6d 65 74 61 0a 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 63 61 70 61 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 79 65 73 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 45 72 69 20 47 6c 6f 62 61 6c 20 49 6e 63 22 3e 3c 74 69 74 6c 65 3e 57 65 6c 63 6f 6d 65 20 74 6f 20 45 72 69 20 47 6c 6f 62 61 6c 20 49 6e 63 2e 20 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 48 65 61 6c 74 68 63 61 72 65 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 4c 6f 62 61 6c 20 48 65 61 64 71 75 61 72 74 65 72 73 20 2d 20 4e 65 77 20 59 6f 72 6b 2c 20 4e 2e 59 2e 20 57 48 59 20 45 52 49 20 47 4c 4f 42 41 4c 20 49 53 20 54 52 41 4e 53 46 4f 52 4d 49 4e 47 20 48 45 41 4c 54 48 43 41 52 45 57 6f 72 6b 69 6e 67 20 6f 6e 20 62 65 68 61 6c 66 20 6f 66 20 6f 75 72 20 43 6c 69 65 6e 74 2d 62 61 73 65 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 70 61 67 65 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d Data Ascii: 2a60<!DOCTYPE html><htmllang="en-US" xml:lang="en-US" prefix="og: http://ogp.me/ns# fb: http://ogp .me/ns/fb#"><head><metahttp-equiv="Content-Type" content="text/html; charset=UTF-8" /><basehref="//eriglobal.com/" /> <metahttp-equiv="x-ua-compatible" content="ie=edge" /><metaname="apple-mobile-web-app-capable" content="yes" /> <metaname="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" /><met aname="apple-mobile-web-app-title" content="Eri Global Inc"><title>Welcome to Eri Global Inc. Transforming Hea lthcare</title><metaname="description" content="GLobal Headquarters - New York, N.Y. WHY ERI GLOBAL IS TRANSFO RMING HEALTHCAREWorking on behalf of our Client-base" /><metaname="page-type" content=
Feb 3, 2021 19:50:17.037497997 CET	2168	OUT	GET /css/plugins/menu.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:17.201086998 CET	2170	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:14 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:56:33 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:14 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 1481 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 cd 58 fb 6e ab 36 18 ff ff 3c 05 6b 34 a9 39 0b 39 40 92 5e 40 ab f6 00 9b 8e 34 69 0f e0 80 93 58 25 18 81 69 d3 46 7d f7 7d be 00 c6 d8 34 55 3b 69 ad 5a 01 36 df e5 e7 df 77 63 96 d6 f5 11 17 cd f9 88 aa 3d 29 e2 cd a6 3c 79 41 52 a2 2c 23 c5 3e 0e 92 2d ad 32 5c c1 45 4e 6a e6 d7 ec 25 c7 71 41 0b 0c f7 05 f6 0f 98 ec 0f 2c 0e 93 8c d4 65 8e 5e e2 6d 4e d3 c7 a4 a4 35 61 84 16 71 85 73 c4 c8 13 7e 9b 29 3d 5e 93 b7 aa be 5e 4b c2 f0 89 f9 28 27 fb 22 4e 71 c1 70 a5 eb f5 72 f2 05 aa 49 21 9e 5f e0 27 e8 f3 50 a7 d1 5b 97 a7 af 77 b8 15 18 06 70 6c 5c c3 8e 16 20 8e bc e2 38 bc 81 5b 01 48 86 53 5a 21 f1 a2 50 91 d2 9c 56 f1 2c 08 02 b9 7d 87 8e 24 7f 89 af 7e d6 cf 28 cf ae 16 35 2a 6a bf c6 15 d9 8d dc 89 0f f4 09 57 67 69 bd bf a5 8c d1 63 1c 81 ee 9a e6 24 f3 66 51 78 7b 97 a2 d1 6b 4b 94 b2 06 e5 7e 89 f6 f8 f2 97 67 fc bf bf 6d 60 5f f1 1f 92 c6 7f c6 db 47 c2 c0 a0 13 47 8e cb ee 4c 3c 25 fe 91 be 3a 96 ac 4f 3b f3 63 b4 03 02 2e da db 87 26 97 4f ce 29 60 0e e4 8c af 96 57 86 6d 69 8e 51 05 b2 d8 21 79 22 35 d9 92 9c b0 97 f8 40 b2 0c 17 03 a7 82 a4 bd 70 a0 d5 ca e5 70 74 5b 96 22 32 7c 19 19 60 cf b9 27 4b 30 11 3a e6 6b 0f 10 47 d6 68 d8 e5 14 b1 09 95 9c 0d a0 55 d3 94 e3 1d 33 f7 56 dc 31 a5 46 4a 14 4f de 34 20 61 e9 01 9d ad dc 16 0f 59 05 0c de d1 ea 18 37 65 89 ab 14 d5 c3 c0 04 23 3a 1a a0 2d b0 af 61 40 1a b0 25 f6 ef e1 a7 3c 59 6d 1a 9b 3f 34 4c ae f3 2c d3 9d 52 4b 2d 61 90 d2 97 e7 de 32 da d4 1e 06 ab 24 bb 26 56 eb 89 45 ea 5e 73 2d f4 b6 e6 44 86 32 a7 81 f0 1c 35 8c da dd b6 6e 4d 2a 93 7f da b6 87 1e 83 d5 46 43 53 21 d4 95 00 5f 88 0b 83 e0 d7 84 d1 52 13 36 86 dd 7c 29 48 d4 9d b4 83 cb 18 1f 04 a4 5f 95 23 38 37 bc 5f c8 b1 a4 15 43 05 eb f3 66 08 e9 27 04 1b 93 67 92 b1 43 1c 6d 82 61 12 5d 5f 9a 44 9f a5 bf 6b b8 df a2 f4 71 5f d1 a6 c8 e2 6a bf 45 d7 d1 66 b3 68 ff 82 e5 dd 3c 79 f5 49 91 e1 53 cc c9 76 6f 52 36 45 25 61 e0 ff eb c0 60 57 d0 74 be 2a f0 d1 c2 82 82 ca da ca 64 4b 8e 16 fb 96 07 04 69 bf d9 3e 20 95 a8 5c d8 8d 42 87 1f 9e 28 37 ea 30 c2 0e cf 3b b8 52 4c 80 44 6f a4 3b 0d a7 59 96 65 49 97 18 af a6 88 60 31 54 aa 15 b4 94 8c 0a c7 a4 1b bc b6 c5 00 35 b6 24 01 e1 c9 aa f7 64 3d 32 5a f1 a4 f7 8b bb e8 f6 e4 ff 9b 02 de 83 56 61 34 c2 76 3d c2 f6 a1 7f af 65 61 fb b6 c0 f3 b6 07 2b 78 fb e3 88 33 82 3c 6e 13 2a 32 ef fa 88 4e be c4 d4 bb bd 01 2c e7 0b 8f 16 f9 8b 57 a7 15 Data Ascii: Xn6<k499@^@4iX%iF}}4U;iZ6wc=)<yAR,#>-2\ENj%qA,e^mN5aqs~)=^^K("'NqprI!_'P[wpl\ 8[HSZ!PV,}$~ (5*jWgic$fQx{kK~gm`_GGL<%:O;c.&O)`WmiQ!y"5@ppt["2|``K0:kGhU3V1FJO4 aY7e#:-a@%<Ym?4L,RK-a2$&VE^s-D2 5nM*FCS!_R6|)H_#87_Cf'gCma]_Dkq_jEfh<yISvoR6E%a`Wt*dKi> \B(70;RLDo;YeI`1T5$d=2ZVa4v=ea+x3<n*2N,W
Feb 3, 2021 19:50:18.633975029 CET	2326	OUT	GET /css/plugins/share.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:18.797108889 CET	2329	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:16 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:56:34 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:16 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 768 Keep-Alive: timeout=20, max=298 Connection: Keep-Alive Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 8d 97 cd 72 9b 30 10 80 5f 85 63 72 c0 01 99 1f 83 a7 87 3e 41 9f 41 80 8c 35 16 12 95 44 62 37 d3 77 af 0c b2 eb 14 ed ba 9e 1c 00 ef c7 e7 15 bb 8b b2 31 47 aa 59 4c 0f 07 7e fe 1c 95 e1 96 2b 59 bb 13 d6 ed ad 1a eb 3c 19 cf 7b c1 0e b6 4e 7e 6f 96 58 de 2a f9 d9 d0 f6 d4 6b 35 c9 2e d6 6c 64 d4 d6 52 f9 a3 fd c3 77 7c a0 3d ab 27 2d 5e 36 9b 37 f7 37 9f 9b 37 a3 5a 4e c5 7c 27 b3 19 65 ff ba 3f 32 de 1f 6d 9d 5d 75 1f bc b3 c7 e5 b0 e3 66 14 f4 52 73 29 b8 64 71 23 54 7b da 5b 76 b6 31 97 1d 93 b6 8e ab eb c7 45 0e 54 f7 5c d6 c4 1d aa 91 b6 dc 5e ea 4d b5 3f 70 61 99 ae bf 8b f1 48 5f 7e 2c d7 bf 55 c9 eb 63 2e f5 51 bd 33 fd 79 a3 d2 30 94 26 5f a9 b8 e3 7d ff b8 0c f7 c5 8b 73 52 8c e7 e8 cb 7a c5 6c a0 5c 84 c3 8b 34 5b 85 1f 04 6f 4f 3a 1c 4f 8a 74 1d af 26 6d 7e 4e ee 3c c8 24 ff 84 6b 63 c2 f7 de 26 f9 fa de b4 65 8d 52 a7 30 91 6e d7 bf c6 7e 70 eb 56 10 00 ca 75 ba 76 1a 1a 01 c4 ef ca 55 b8 ab 85 13 eb b8 0c 03 d9 76 b7 22 de f9 c0 14 90 72 b5 5d 85 73 69 2c ed 35 1d 00 c3 3a 83 91 4b 97 31 33 16 90 64 d5 0a e9 95 ea 05 1b c5 04 3c 0b 92 ae f3 e0 32 05 7e d2 8e ac 82 cd bc ac 6c 1a 15 b0 52 79 99 3c 42 be 80 e2 41 fd 8a ad a6 d2 87 51 21 a2 0d 31 d1 b5 03 a9 8e 12 f3 d0 e0 ff d1 da d1 7d 30 44 a6 d5 ca dd ec 3a 4e 22 37 5c a2 59 32 3a a7 b4 e1 4e f7 53 61 7b ed ea f9 b2 bf 90 3c b6 fb 32 2e ae 31 5f 13 89 1b 76 a4 b2 0d 77 44 9c cf 0f 71 7e 94 61 cc 8f 05 0c 2e cb 15 dc 31 d7 b9 5c 41 cf 34 4f 09 60 bd 83 a8 77 c1 83 de 77 4e a5 a5 1a 28 c0 6c 97 80 e2 1b 89 99 3d 1f 32 83 73 30 cb 76 90 d3 31 a8 6d 21 43 36 cd 9b c6 15 35 c0 a5 05 64 f4 1c 6a 5d e8 80 15 9b de 25 54 47 33 84 f9 3c 1a f0 e1 23 77 bb 83 94 37 0e b3 7a 3a 64 45 5e 3a db 1c 2a dc 85 42 8d 39 54 b5 07 a5 35 38 32 09 54 b1 0b 85 1a 09 54 ad 4f 87 ee 0e aa d9 bf 24 66 f6 7c c0 0c 8e ee bc 84 8a d6 21 e8 34 28 a1 7a 7d f2 fe 2a 12 28 c9 3b 88 d6 6d 02 e5 28 a8 b1 07 40 4a 72 28 cd 85 42 57 35 87 32 c5 b7 02 84 40 9d 72 e3 50 2b 81 3a e5 c9 db 3e ad a0 66 b9 83 98 d7 e3 01 2f b8 6f 4b 0b a8 59 1c 82 ba 0a a8 53 cc e9 32 02 63 36 25 50 fd cc 10 ea 23 50 ed 3c dd ad 14 19 94 e3 03 8a d6 6d 06 e5 8a ed 3f 2b a8 6c 17 08 13 56 50 d5 a2 1b e4 02 aa 59 4f e1 29 02 46 6c 03 0c 15 eb cc e0 63 16 b0 5d d4 64 a7 06 fa 5f 24 e4 f2 04 62 4b bc e9 0f 8e 98 af e5 b2 0e 00 00 Data Ascii: r0_cr>AA5Db7w1GYL~+Y<{N~oX*k5.ldRw|='-^6777ZN|'e?2m]ufRs)dq#T{[v1ET\^M?paH_~,Uc.Q3y0&_}s Rzl\4[oO:Ot&m~N<$kc&eR0n~pVuvUv"r]si,5:K13d<2~lRy<BAQ!1}0D:N"7\Y2:NSa{<2.1_vwDq~a.1\A4O`wwN(l=2s0v1m !C65dj]%TG3<#w7z:dE^:*B9T582TTO$f|!4(z}*(;m(@Jr(BW52@rP+:>f/oKYS2c6%P#P<m?+lVPYO)Flc]d_$bK
Feb 3, 2021 19:50:19.429390907 CET	2357	OUT	GET /css/fonts/oswald-regular.woff2 HTTP/1.1 Host: eriglobal.com Connection: keep-alive Origin: http://eriglobal.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://eriglobal.com/css/default.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.592540979 CET	2429	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:55:53 GMT Accept-Ranges: bytes Content-Length: 21196 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=297 Connection: Keep-Alive Content-Type: font/woff2 Data Raw: 77 4f 46 32 00 01 00 00 00 00 52 cc 00 12 00 00 00 00 c7 00 00 00 52 65 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 46 46 54 4d 1c 1a 28 1b a3 1c 1c 24 06 56 00 86 6e 08 2e 09 92 62 11 08 0a 82 ac 6c 82 8e 48 01 36 02 24 03 8d 0c 0b 86 48 00 04 20 05 8a 07 07 20 0c 81 05 1b 59 b3 35 e2 6d 17 c4 ed 00 fd d8 d7 7f a6 d9 88 18 9c 07 a2 85 f8 fd d2 c8 40 b0 71 80 81 3f ef 9a fd ff 9f 13 e4 18 a3 0d bf 03 c5 ea 2b 11 91 19 22 ac 66 59 39 0b a5 cd aa a2 f7 49 09 66 b3 85 27 56 57 de 34 a8 b2 40 ad ff 0c 21 84 90 10 5d 7e 56 65 dc c7 6f f4 dc 9e 20 3c 1d 27 fe 53 cf ab fa c9 77 46 b3 0d 47 d0 9e 3a 29 47 19 7e 99 82 a1 3d d4 ce 0a d7 1b de 1c ed e5 1e de 2b ed 33 04 c6 08 40 00 e3 f3 89 5a 3b 6a 55 54 e2 28 8b c0 b8 85 8f 9a 53 af 5f ef cf 3e cf e9 ee 0b 0f 50 34 a3 37 b4 d2 b0 3e b2 ee ae 19 9f 81 28 73 15 41 6a c7 2e 87 4e 17 73 13 04 89 b3 c4 3f f0 73 eb fd bf 35 03 b6 51 a3 c6 c8 11 39 2a f6 61 83 11 39 36 46 0c 18 d5 8a 0c b1 d8 b7 11 30 4f 05 41 10 0b 23 51 41 7b df 38 2c b4 2f 3d 0f fb a2 8c be 3b 3f cf 7f ad fd bf 6b f7 e9 9e b9 2f 80 8e 50 12 aa b0 4a f9 28 24 87 ea 83 4f 3c 91 23 b2 a9 08 1f 56 5f 05 48 02 cd eb e3 f7 57 31 6d 6a bb 19 2e e1 c7 55 53 48 f2 c1 7c 07 cf ad fd 65 33 73 f9 f0 8e 51 32 e7 18 5a be a4 84 5f b2 fe 53 cd aa aa bb 7f 40 a0 44 0c 35 c9 31 d0 31 82 d4 66 3d 2d 97 9c 80 81 83 7c d1 c2 e3 fb d5 47 07 c0 64 5d ff 25 dd cb 64 69 4e 35 16 c0 c9 9f be 79 d8 18 b8 07 d0 83 d3 c9 e0 4b 87 eb d2 97 c6 7e db 37 c1 6d ec be ec 75 48 fa b8 50 c0 db 1d d2 8a 86 58 a1 22 cf 7d 49 26 62 5e e7 de a0 5b 15 b0 8a 85 18 41 06 0d c1 46 6d 2d 67 22 d5 7d d3 7f 57 ed 69 01 fc fb ff da fa fd 8f f7 62 41 6e 78 88 cd 20 f6 25 58 76 bd 9a 5d 2c 0f cd ac d5 34 25 27 5d 75 df e0 7d 85 ff cd 96 17 6b fa 37 5b c5 f8 c8 89 55 71 ed 81 75 fd 53 f5 15 0f 6 0 91 f0 f0 c4 fb cb 60 3b c9 9e 69 f0 85 ec d2 a7 4b 29 a0 b0 80 76 07 be 32 d5 da 54 2e 73 36 97 3d e5 ef 4d b5 4a ff ff 34 d3 d4 8c 54 34 6b e4 02 6a b7 b0 05 ae d7 ac 89 45 ad b4 d6 9c 71 41 7e 59 f7 fb bf d1 ed 09 34 00 aa d5 10 44 10 10 75 24 38 d2 01 34 fe 58 ec 06 a8 c5 80 e4 14 87 e4 58 ce 55 69 8d f3 00 64 4e 04 65 29 73 de da 24 bd ec 2e dc ec 5c 96 d8 e8 b2 ab fc 82 20 be 20 5c f8 e7 db af d5 b9 8b c7 0d f1 37 ea 0f 11 6a fa cc 62 6f dd e3 0e 6a c9 3c e3 a7 5b 88 78 25 11 2b a1 10 2a 14 e5 c9 01 dc 89 9c e8 bb 45 db 88 14 50 fb bf 53 93 7e e9 7f 35 7e 76 97 3a d6 02 f8 92 6e 36 26 c0 05 c8 51 ec 28 89 f4 73 d7 35 87 cf d7 57 5f e7 46 b0 9b 1d 20 ac 14 16 fa 2e c6 37 6f d5 a2 a2 dc e7 24 eb fe aa 95 e9 3e 3f 6f ec 64 37 e5 6d b2 a9 7b 0d bd 70 04 Data Ascii: wOF2RRe?FFTM($Vn.blH6$H Y5m@q?+"fY9If'VW4@!]~Veo <'SwFG:)G~=+3@Z;jUT(S_>P47>(sAj.Ns?s5Q 9*a96F0OA#QA{8,/=;?k/PJ($O<#V_HW1mj.USH|e3sQ2Z_S@D511f=-|Gd]%diN5yK~7muHPX"}I&b^[AFm-g"}WibAnx %Xv],4%']u}k7[UquS``;iK)v2T.s6=MJ4T4kjEqA~Y4Du$84XXUidNe)s$.\ \7jboj<[x%+*EPS~5~v:n6&Q(s5W_F .7o$>?od7m{ p
Feb 3, 2021 19:50:19.820437908 CET	2544	OUT	GET /images/building.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.983721018 CET	2640	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:20 GMT Accept-Ranges: bytes Content-Length: 29099 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=296 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 38 42 41 30 32 46 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 38 42 41 30 32 45 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:248BA02F33B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:248BA02E33B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:
Feb 3, 2021 19:50:20.153726101 CET	2808	OUT	GET /images/header-BG.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/css/custom.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.317225933 CET	3009	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:49 GMT Accept-Ranges: bytes Content-Length: 1279 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=295 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 34 36 35 32 44 39 43 36 33 33 42 33 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 34 36 35 32 44 39 43 35 33 33 42 33 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:4652D9C633B311E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:4652D9C533B311E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:8
Feb 3, 2021 19:50:20.348817110 CET	3077	OUT	GET /images/b-bullet.png HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/css/custom.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.512614012 CET	3302	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:49:57 GMT Accept-Ranges: bytes Content-Length: 1396 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=294 Connection: Keep-Alive Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 01 68 f4 cf f7 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 28 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 43 32 35 42 33 44 31 42 33 33 42 41 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 43 32 35 42 33 44 31 43 33 33 42 41 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 43 32 35 42 33 44 31 39 33 33 42 41 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 43 32 35 42 33 44 41 31 41 33 33 42 41 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d Data Ascii: PNGIHDRhtEXtSoftwareAdobe ImageReadyqe<(iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0 MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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 2019 (Macintosh)" xmpMM:In stanceID="xmp.iid:C25B3D1B33BA11E99802BA97030217B8" xmpMM:DocumentID="xmp.did:C25B3D1C33BA 11E99802BA97030217B8"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:C25B3D1933BA11E99802BA97030217B8" stRef:documentID="xmp.did:C25B3D1A33BA11E99802BA97030217B8"/> </rdf:Description> </rdf:RDF> </x:xm

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49936	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:51:02.778630972 CET	7312	OUT	GET / HTTP/1.1 Host: eriglobal.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english; _ga=GA1.2.406443051.1612410619; _gid=GA1.2.696941932.1612410619
Feb 3, 2021 19:51:03.141500950 CET	7328	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:51:00 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=20, max=300 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:51:04.570453882 CET	7377	OUT	GET /uploads/videos/c4ca4238a0b923820dcc509a6f75849b/videoplayback-1558705888.mp4 HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: identity;q=1, *;q=0 Accept: */* Referer: http://eriglobal.com/ Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english; _ga=GA1.2.406443051.1612410619; _gid=GA1.2.696941932.1612410619 Range: bytes=339316-16811172 If-Range: Fri, 24 May 2019 13:51:28 GMT
Feb 3, 2021 19:51:04.737643003 CET	7379	IN	HTTP/1.1 206 Partial Content Date: Wed, 03 Feb 2021 18:51:02 GMT Server: Apache Last-Modified: Fri, 24 May 2019 13:51:28 GMT Accept-Ranges: bytes Content-Length: 16471857 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:51:02 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Range: bytes 339316-16811172/16811173 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: video/mp4 Data Raw: dc 31 c3 69 78 2b e6 e2 24 a1 15 78 2d 7c f5 94 10 6f 29 de 32 d5 de 51 71 d7 7b 07 25 c6 ac b3 56 89 fa e1 16 10 bb e8 ce e1 78 c8 6d ff e8 e4 f0 64 95 2e e2 08 b9 6b 82 74 b9 b4 85 f8 02 d6 76 ad a0 01 12 41 4e d9 25 7e a7 5f 15 4e ad cf 08 a7 66 29 48 cd 6b ed 6e a3 32 9c 33 f4 7d d6 c5 ae ec 9b 09 31 43 50 50 a0 a9 9f 39 2b 99 7f ad 8a b5 ad a6 56 9a 2c af de 60 91 6e 16 4c a3 e1 23 4f 0a 9f 19 1e c3 e8 0b 79 22 7d 68 a3 a7 d3 25 6f 92 e0 1c 67 46 1a e0 08 84 2d 9c 8d 7a b4 05 86 2c c7 5f 0b 8e 48 8c a8 03 cc bf be 0e 54 9c 26 f5 78 c5 30 46 3d f1 58 2d 05 a5 be dc 33 b1 41 c7 cb 36 39 c1 4f 5b 19 e8 76 84 44 f0 6b fb b5 21 81 b9 5b 0a 9a 72 82 39 0c 76 8e f4 16 a3 2b a8 f0 d5 b6 5c 91 74 65 a2 38 7e 09 a0 18 2c da d4 91 65 78 02 b5 5b 3e b7 df fc 0c 23 cd 10 1e eb 3b e3 fb 41 f9 20 40 72 9b 45 6f a8 19 c9 55 81 43 e7 2a 63 30 c0 b0 7d e2 17 2c ad a1 45 ec 84 c1 f0 26 d4 fa 29 7f 67 c0 e4 66 87 12 f9 dc 64 ee 8a 99 62 6c aa 73 6f cd 9d 77 32 3d e6 bc aa 93 18 dc 40 c3 a4 a9 cc e2 4e a1 3b b9 80 bf cd b5 bf e5 49 01 fe c1 af f6 30 6d 71 09 b2 4c b1 fc 50 5e 9d 8e 78 d1 c0 06 fa 41 48 5e 23 94 21 49 ea 30 74 90 95 f2 0f 0e d4 7d fd d8 7b 6a 46 5a fe 70 80 34 f6 6a 43 87 0e 43 17 1e f6 89 ef e3 c8 a9 ec 04 cc 40 72 53 e8 68 d2 d0 aa f4 72 c5 db ee 4d 7c 63 59 7e 2b 9b c3 20 90 cc f8 6c b2 24 26 51 05 8d a4 50 e8 64 a3 74 b7 25 39 b8 04 26 d1 9b f4 cd 9d 80 cd 7d e4 3c 51 61 13 7e 55 92 c0 07 3b 60 06 6f 05 7a 8c 7d 24 4d a5 67 18 32 7e a9 41 12 56 6a a0 e0 92 e0 55 97 f1 b8 8c 8c 28 6b 08 c5 fc af ca 17 66 5a bb bd 4b d9 1b 57 0e e0 62 3e 36 ce 32 d1 c8 d6 22 d2 4e 6e 31 bd 80 cd 9b c3 53 be 05 e0 1d fe c7 8b 95 44 69 56 c2 ac d2 c3 71 f6 b9 ad e3 a0 25 a3 9d 2b f4 5b 0e 55 83 86 a0 1d 16 f2 61 21 7d a7 40 af 04 98 85 df 8b 71 38 ba e7 06 51 f3 ea 22 22 bb 53 86 c5 06 e3 10 04 3f 91 ea 50 d0 76 b2 e0 b0 cb a5 1c c3 98 48 6a cf 9f 7d 9e 62 3c 88 36 b7 bc bc 4d 90 bd f0 fd 2c 63 5e 33 ab df 80 b5 01 62 e3 a0 54 bc 93 62 e0 c8 fc dd 9f 01 1f c1 ff 4f 1d 93 c6 da 40 0e 47 e5 83 78 ae 61 28 43 a7 b9 6c 53 cc 78 6d de 99 19 52 82 40 94 e8 05 fa fd 0f 79 3e fa be 1d 44 76 ea a4 e7 ce 54 88 7f 79 4d 45 0f cd 35 66 1c 1d 3a 0c 03 fa 92 d2 49 98 c4 77 1b 2a 92 d2 9b e7 8a 35 3d 5f 2f 43 8a 79 74 86 a6 a1 9c d3 f6 49 a8 02 e2 8d f5 e1 bb 9f 0a 34 a1 ef f1 f2 b8 80 cf f7 a2 c4 d0 88 55 16 e7 4c 96 bb 63 5c 13 4e 7f c3 f9 1e 2b 76 dd 5c 11 2a ad 0e f2 60 ff 24 Data Ascii: 1ix+$x-\|o)2Qq{%Vxmd.ktvAN%~_Nf)Hkn23}1CPP9+V,`nL#Oy"}h%ogF-z,_HT&x0F=X-3A69O[vDk![r9v+\t e8~,ex[>#;A @rEoUC*c0},E&)gfdblsow2=@N;I0mqLP^xAH^#!I0t}{jFZp4jCC@rShrM\|cY~+ l$&QPdt%9&}<Qa~U;`oz}$M g2~AVjU(kfZKWb>62"Nn1SDiVq%+[Ua!}@q8Q""S?PvHj}b<6M,c^3bTbO@Gxa(ClSxmR@y>DvTyME5f:Iw*5=_/Cy tI4ULc\N+v*`$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49935	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:51:08.900518894 CET	7501	OUT	GET / HTTP/1.1 Host: eriglobal.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english; _ga=GA1.2.406443051.1612410619; _gid=GA1.2.696941932.1612410619

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:51:09.256922007 CET	7503	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:51:06 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=20, max=300 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 61 36 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 0a 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 66 62 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 2f 66 62 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 0a 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 3c 62 61 73 65 0a 68 72 65 66 3d 22 2f 2f 65 72 69 67 6c 6f 62 61 6c 2e 63 6f 6d 2f 22 20 2f 3e 3c 6d 65 74 61 0a 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 63 61 70 61 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 79 65 73 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 63 61 70 61 62 6c 65 2d 73 74 61 74 75 73 2d 62 61 72 2d 73 74 79 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 64 65 66 61 75 6c 74 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 45 72 69 20 47 6c 6f 62 61 6c 20 49 6e 63 22 3e 3c 74 69 74 6c 65 3e 57 65 6c 63 6f 6d 65 20 74 6f 20 45 72 69 20 47 6c 6f 62 61 6c 20 49 6e 63 2e 20 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 48 65 61 6c 74 68 63 61 72 65 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 4c 6f 62 61 6c 20 48 65 61 64 71 75 61 72 74 65 72 73 20 2d 20 4e 65 77 20 59 6f 72 6b 2c 20 4e 2e 59 2e 20 57 48 59 20 45 52 49 20 47 4c 4f 42 41 4c 20 49 53 20 54 52 41 4e 53 46 4f 52 4d 49 4e 47 20 48 45 41 4c 54 48 43 41 52 45 57 6f 72 6b 69 6e 67 20 6f 6e 20 62 65 68 61 6c 66 20 6f 66 20 6f 75 72 20 43 6c 69 65 6e 74 2d 62 61 73 65 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 70 61 67 65 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 64 6f 63 75 6d 65 6e 74 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 2c 6e 6f 6f 64 70 22 20 2f 3e 3c 6d 65 74 61 0a 6e 61 6d 65 3d 22 63 6f 70 79 72 69 67 68 74 22 20 63 6f 6e 74 65 6e 74 3d 22 22 20 2f 3e 3c 6d 65 74 61 0a 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 57 65 6c 63 6f 6d 65 20 74 6f 20 45 72 69 20 47 6c 6f 62 61 6c 20 49 6e 63 2e 20 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 48 65 61 6c 74 68 63 61 72 65 22 20 2f 3e 3c 6d 65 74 61 0a 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 4c 6f 62 61 Data Ascii: 2a60<!DOCTYPE html><htmllang="en-US" xml:lang="en-US" prefix="og: http://ogp.me/ns# fb: http://ogp .me/ns/fb#"><head><metahttp-equiv="Content-Type" content="text/html; charset=UTF-8" /><basehref="//eriglobal.com/" /> <metahttp-equiv="x-ua-compatible" content="ie=edge" /><metaname="apple-mobile-web-app-capable" content="yes" /> <metaname="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" /><met aname="apple-mobile-web-app-title" content="Eri Global Inc"><title>Welcome to Eri Global Inc. Transforming Hea lthcare</title><metaname="description" content="GLobal Headquarters - New York, N.Y. WHY ERI GLOBAL IS TRANSFO RMING HEALTHCAREWorking on behalf of our Client-base" /><metaname="page-type" content="document" /> metaname="robots" content=",noodp" /><metaname="copyright" content="" /><metaproperty="og:title" content="Welcome to Eri Global Inc. Transforming Healthcare" /><metaproperty="og:description" content="GLoba
Feb 3, 2021 19:51:09.949124098 CET	7514	OUT	GET /uploads/videos/c4ca4238a0b923820dcc509a6f75849b/videoplayback-1558705888.mp4 HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: identity;q=1, *;q=0 Accept: */* Referer: http://eriglobal.com/ Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english; _ga=GA1.2.406443051.1612410619; _gid=GA1.2.696941932.1612410619 Range: bytes=408351-16811172 If-Range: Fri, 24 May 2019 13:51:28 GMT

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:51:10.114324093 CET	7515	IN	HTTP/1.1 206 Partial Content Date: Wed, 03 Feb 2021 18:51:07 GMT Server: Apache Last-Modified: Fri, 24 May 2019 13:51:28 GMT Accept-Ranges: bytes Content-Length: 16402822 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:51:07 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Range: bytes 408351-16811172/16811173 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: video/mp4 Data Raw: 66 69 77 8f 9f ec ec 59 e9 3e 25 be b9 c9 ff 28 11 ee cd 8a 9f 5b da d2 7c af 68 a7 f2 cd c6 15 4e 5e 5a fa 30 b0 78 27 42 65 ec 1d 80 a2 4f 8d 77 18 17 ba a6 66 34 90 1d b9 b2 97 22 cc 1c f3 41 ab 4b ba 6d 60 3a 6d 74 8a 33 6b 02 9c 34 a5 69 66 a9 1f bc 1b 94 ed 80 48 6e 25 3b 80 33 1b 19 53 c9 04 67 a5 19 4a 68 ed 6e 08 7d 82 ea c8 34 7c 44 17 9d b5 1c e4 b9 6b 02 74 49 24 87 75 5a a9 12 71 47 33 b6 ac 21 a2 ae 0b d8 09 e0 a2 5b 3b 3b d5 40 37 d5 0e d0 ff ca 99 14 e3 7c 5b a0 33 8e d6 4e 47 3a 30 a5 d4 37 97 63 70 80 8a ef b5 eb 70 08 18 68 de 70 9c 71 60 31 9f d6 81 01 6c f7 4c f0 c9 0a 4a 4f f7 3f 6e 33 bd fb ea 0c be 68 1b e5 83 5d e3 bf 26 8f 73 1b c0 e4 1a 65 37 2c ff 3b 70 bb 79 f4 7a c9 57 d2 98 44 51 09 12 50 ae 0f ef 34 c6 7c 74 03 94 1a 50 bc 8b ee 30 50 f4 fd 7e 27 50 b7 88 58 0c dd 55 13 07 61 7d 35 26 7a 8f 3c 16 86 c6 fb 24 ec f5 af 4f 9f 64 a1 51 32 aa ec 5f 66 12 d7 5c e5 00 37 55 a7 85 5f 3e e3 1a 9e 21 c6 6c 99 1d 5c 61 1b 39 de 21 7e 46 88 94 ad cc d5 bc 25 8c ba 38 ac 9e 34 a7 ac 50 82 cf 33 cd cc 40 d9 ac 40 fd 1b 7d 92 30 7e 82 64 d3 9b 72 19 4a 6f 6b b5 f6 02 5d 69 e6 e4 65 dd cb 92 e1 90 67 e0 09 6b 8a ac c9 0f 4a bc 4f 4b 4a f1 53 eb 47 23 97 92 c3 1e 34 e3 62 f6 2d ae 11 82 67 b1 90 0e 36 78 03 47 57 63 66 3f 8c 9b 9a c3 38 34 51 e7 a3 28 43 bc 56 90 74 e4 0b c5 c3 14 4b 35 9c 5d 04 d1 c0 66 cc e1 e3 ce c1 0d 94 ad 8c d2 a2 ba 6d bf 0d e7 2e 72 57 ea e4 6f 3a 24 e3 7a d1 de f3 cc 5f 0f 89 52 f0 1c 67 2c 7d d2 a3 36 cf f2 93 3a 48 03 97 d5 34 b8 b5 4f 27 9d bb 30 5f 6e c3 20 b9 9d 3e c9 3f 08 f8 49 3e 1e 1e a1 8b 22 ff 70 bb 0a 1c 0f da 83 ed 87 97 bd 58 91 d5 ae fc eb 63 b6 bc cd 2f 94 cd 3a 48 28 0d 44 5f 10 24 9a cb 31 6c 7a 97 1e ad 76 20 20 ca 5b 7e bc 2f f6 26 d8 9a f7 fd 61 2d d5 69 39 82 6d fe 7b d1 53 8a 87 23 94 ba ec 66 f6 62 ee 18 48 31 5e d0 69 10 a1 e4 d2 4d e2 0c 63 80 1f d8 62 bc 09 4e 9c d9 88 b6 55 ac 11 21 e8 f0 8e 6e aa 1f e7 f0 c8 ae ef ac 7e 3b 5f 73 56 37 fa f0 ee c1 20 bc a3 4f 49 3d 70 b2 99 04 1a 9d 29 14 b9 a8 91 c0 35 0e a1 c0 69 6a 56 f4 a8 8a 6a 5c 58 a7 a5 c1 a9 75 47 b7 54 12 76 d4 59 d1 34 71 41 2e 0b be f3 a4 5a 82 16 33 16 9e c7 1a 52 d8 5b df 70 56 05 5e c1 34 0e 85 ef d8 c3 7a 76 08 26 39 59 2a 3d 14 21 1b 4a de 0e 04 1e d5 0a c9 a9 e4 ac 7a 2e 06 50 54 e7 e8 c3 88 0e 93 36 59 ce 6f 52 0f e8 dc 13 d6 b1 73 0e 05 c3 3d 15 3f 8e b1 d0 b0 af 72 05 09 90 e5 60 97 37 c9 35 d9 46 76 70 6a d4 Data Ascii: fiwY>%([]hN^Z0x'BeOwf4"AKm`:mt3k4ifHn%;3SgJhn}4|Dktl$uZqG3![;;@7|[3NG:07cpphpq`1lLJO?n3h]&se7,;pyzWDQP4|tP0P~'PXUa}5&z<$OdQ2_f\7U_>!l\a9!~F%84P3@@}0~drJok]iegkJOKJSG#4b-g6xGWcf?84Q(CVtK5]f m.rWo:$z_Rg,}6:H4O'0_n >?l>"pXc/:H(D_$1lzv [~/&a-i9m{S#fbH1^iMcbNU!n~;_sV7 OI=p)5ijVj\XuGTvY4qA.Z3R [pV^4zv&9Y*=!Jz.PT6YoRs=?r`75Fvpj

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49773	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:17.211906910 CET	2171	OUT	GET /css/default.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:17.379560947 CET	2173	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:14 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 04 Mar 2019 19:50:11 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:14 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 14869 Keep-Alive: timeout=20, max=300 Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d fb 93 e3 b8 91 e6 ef fb 57 e8 aa af 6f ba e6 44 8d 48 3d 4a aa 8a d9 f5 d8 be b9 73 c4 7a 37 c2 f6 46 d8 e7 9b 73 80 24 24 71 8a 22 69 3e ea 31 8a fa df 0f 2f 22 01 30 c1 92 aa ab 1d e3 5b 8f a6 bb 25 22 f1 fe 00 24 32 3f 80 5f 9f 82 47 1a df 67 6d 10 97 4f 41 93 fd 94 15 fb db b8 ac 53 5a f3 27 77 c1 b1 fc c9 13 84 3f 2d bb 36 cf 0a 7a 5b 94 05 7d f9 fa 36 a6 bb b2 a6 d3 af 6f c9 ae a5 f5 17 ce 6c 57 26 5d c3 f3 4a da ec 81 9e cc d0 c9 7f c9 8e 55 59 b7 a4 68 5f 0e ed 31 3f ed ca a2 0d 76 e4 98 e5 cf b7 0d 29 9a a0 a1 75 b6 63 45 68 82 96 3e b5 3c 33 1a 90 f4 c7 ae 69 6f c3 f9 fc e3 5d 5f f4 57 42 49 15 1c b2 fd 21 67 7f da 20 29 f3 b2 be 6d 6b 96 7e 45 6a ca f2 8e cb f4 d9 ca 3b 20 55 95 d3 a0 79 6e 5a 7a 9c ca 7f 82 2e 9b fe 92 15 fd fe b7 24 f9 bd 78 f2 3d 8b 31 bd fa 3d dd 97 74 f2 1f bf b9 9a fe a e 8c cb b6 9c 5e fd 2f 9a 3f d0 36 4b c8 e4 df 68 47 af a6 df d5 19 c9 a7 46 7d 44 56 8f 94 97 e6 36 9a cf e5 6f 5e fa db b0 a6 c7 3b de 3e c1 41 06 87 b3 65 b4 59 dd dc c9 42 7f 58 2c 16 77 47 52 ef b3 e2 76 7e 17 93 e4 7e 5f 97 5d 91 aa 3a 7d d8 ed 76 2f d9 71 7f 3a 92 a7 e0 31 4b db 83 6c 07 fe b3 4f 8f ff 96 9d c5 52 e8 93 e2 91 66 69 d6 90 38 a7 e9 a9 ac 48 92 b5 cf b7 b3 1b fe fc cf 84 35 5b f1 ed 55 4e 77 ed d5 0f 53 fe a4 69 9f 73 fa f5 b7 57 bb bc 24 ed ed c4 1b 22 03 4e 2a 97 55 f5 34 09 f9 5f fc cf dc 4c ba e6 45 c3 d3 f6 07 a9 10 33 f5 f9 a4 cf e3 e5 10 4e 0f d1 f4 b0 98 1e 96 d3 c3 6a 7a 58 9f 04 44 44 af 33 f0 1f 6f bb aa a2 75 42 1a 6a 36 ad db 31 2a ed 68 2e 4a 4c 4e 4a 74 49 b6 73 1a dd 89 14 53 9a 94 35 69 b3 b2 90 80 27 b7 87 f2 81 0d 2a 25 1a 2d 56 d1 4d 32 10 65 7d 46 6b de cf bd fc 84 61 b1 98 c9 ce e4 20 9b aa e7 b3 c7 ac 61 b8 65 88 96 c9 7a f2 14 83 ec dc 3c f5 08 6d 0f 59 31 49 cb b6 a5 a9 7e c6 5b 90 74 6d 39 e9 07 8f 48 3a a8 d9 20 97 28 eb 25 83 72 b7 6b 68 7b 1b 44 ac b9 b3 29 3d ca 11 24 3a e9 36 6b 59 d7 26 2f d5 a9 22 69 ca e7 07 d1 3d 80 b7 59 93 67 ac 34 a7 aa 6c 32 51 38 12 37 65 de b5 f4 ae 2d 2b 08 9f cc b2 23 d9 d3 93 c6 f2 c3 e3 1d 00 f9 e1 60 0e 81 9a 56 94 c1 a2 28 d5 37 33 4c 67 93 b0 e1 ce 92 65 99 38 59 4c f8 b0 31 86 8c 31 5c 5e 0e 94 f0 b2 ea c2 cb df 93 59 5e ee cb 93 12 e4 4d f6 b2 2b cb 56 0b 06 bc 26 4b 86 9c 97 59 52 56 cf 02 ae 4d 9f 48 28 10 d5 43 2f 49 f9 e7 ce 8b 50 63 7e 88 ec f4 26 1a Data Ascii: }WoDH=Jsz7Fs$$q"i>1/"0[%"$2?_GgmOASZ'w?-6z[}6olW&]JUYh_1?v)ucEh><3io]_WBI!g)mk~Ej; UynZ z.$x=1=t^/?6KhGF}DV6o^;>AeYBX,wGRv~~_]:}v/q:1KlORfi8H5[UNwSisW$"N*U4_LE3NjzXDD3ouBj61*h.JLNJtIsS5i'*%-VM2e}Fka aez<mY1I~[tm9H: (%rkh{D)=$:6kY&/"i=Yg4l2Q87e-+#`V(73Lge8YL11\^Y^M+V&KYRVMH(C/IPc~&
Feb 3, 2021 19:50:17.789545059 CET	2243	OUT	GET /css/plugins/bt.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:17.960882902 CET	2275	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:15 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:56:12 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:15 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 21623 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d db 8e 2b c9 71 e0 7b 7f 05 dd c2 c1 cc d1 34 a9 2a 92 c5 4b 0f 46 90 6d ac 60 03 96 1f ec 15 b0 c0 60 16 28 b2 8a dd d4 29 5e b6 c8 3e a7 39 c2 1a fb 11 fb 01 fb 1f fb e6 4f d9 2f d9 bc 67 64 66 e4 8d e4 19 cb b0 35 9a e9 ee aa 8c 7b 64 64 64 54 5e 7e b7 7e ad fb 53 7b 1e 3c fe f1 bf fe 7e b8 78 fc fe e1 77 bb b6 d9 d6 83 63 bf dd 9f 07 7f 7e 18 0c 7e cd fe 3b 18 9c db f7 f3 f0 f4 5a 37 87 2f cf 83 fd 61 df 0e fe 6a bb 3b 1e fa 73 bd 3f 7f cf 5a ac 0e ef de 06 83 ff c9 9a fc fa f9 79 d5 6e 0e 7d fb 44 7f ad 37 e7 b6 17 e8 53 08 44 49 90 56 35 64 b7 69 d7 87 be 3e 6f 0f fb e7 c1 db be 69 fb 6e bb 6f 25 2f f5 f3 e7 ed 69 7b 6e 1b 93 03 2f 0c 45 be 5a f5 3f 9e b7 e7 ae fd c9 e4 7e 7d d8 9f db fd f9 79 f0 38 f8 f6 71 50 9f cf fd b7 ac d9 c7 c1 e3 c7 47 01 7c ec 5b d1 fa cb 2b 21 3b 3c 1d eb 75 fb 4c 1f 0f bf f4 f5 11 51 67 4f a8 3f 0f ca e3 fb e0 74 e8 b6 cd e0 57 cb e5 92 bf 3b d6 2f ed 70 d5 b7 f5 a7 e1 76 7f da 36 04 4f fd f9 b0 6d 04 a9 55 77 58 7f fa 1f 6f 87 b3 a4 78 03 ae f3 6b 5b 4b 15 35 db d3 b1 ab 2f cf 83 73 bd ea da 21 7d d3 f6 c3 97 fe f0 76 94 ad fb a7 c1 76 f7 22 da 47 50 1f 9f 06 af 63 f2 ef 44 34 3f f4 c7 d7 7a 7f 7a 1e 4c 38 67 5f b6 c4 d0 ec 4f de de 68 0c 70 33 4b 98 a8 47 fb fa f3 aa ee 6d be a9 cf c8 16 ab ba 79 09 e8 a7 28 0a d9 92 49 6b b4 1c ae 0f 5d 57 1f 4f 44 20 f9 1b e2 ed 02 f 0 dc 3c a9 5f 5f 95 b3 ad ea f5 27 aa b9 7d 43 91 1d 08 f1 5f 6d 36 1b d7 a1 39 e4 90 d3 25 ce 7a 7e 7d 72 9f 35 7e 39 9a a6 31 91 12 b4 af e7 5d c7 20 58 7f da fe bc dd bf 3c 4b c9 c8 23 aa fd 0d f1 e8 e1 a6 de 6d 3b a2 b6 13 b1 ca f0 d4 f6 db 0d 7d 45 3b 04 b1 fd f6 e5 95 38 7c 39 2a 2b fa 70 f8 a5 5d 7d da 9e 87 bc 17 6f 7f 6e 87 75 f3 a7 b7 13 6d 51 14 1f 58 8b dd 29 f2 f6 f0 b9 ed 37 dd e1 cb f0 74 be 74 44 b5 a7 75 4f 94 4b cc 68 10 a8 8f c3 57 42 bb a3 f4 a5 ea ce 3d e1 f0 58 f7 ad 50 db af 1d e9 b6 fb 57 c2 bf 30 8d 3f 0c 79 40 1e 7e 47 f9 fb bc 6d bf 50 3d b2 b6 c4 39 cf af cf 83 a6 fd bc 5d 93 1e 4c ff a2 2d eb fe bc 5d 77 04 71 4d fd fd 89 b8 5e dd 1d 5e 9e 06 9b ed cb ba 3e d2 b0 c2 7e 7f a3 b4 37 07 d2 43 49 87 e1 fd 88 fc 64 3d e9 69 b0 ab b7 a4 15 f1 e0 a7 c1 a9 5d 53 18 46 51 79 31 eb de 8c ad d5 a1 b9 b0 77 bb ba 7f d9 92 88 55 38 b6 1b d6 c7 23 f1 95 d3 e5 74 6e 77 04 21 fb 39 7c db 3e 0d fe 86 18 f2 d3 1f ea f5 3f b3 47 bf 27 40 4f 83 c7 7f 6e 5f 0e ec e0 8f 7f ff f8 34 f8 a7 c3 ea 70 3e 90 67 7f d7 Data Ascii: }+q{4*KFm``()^>9O/gdf5{dddT^~~S{<~xwc~~;Z7/aj;s?Zyn}D7SDIV5di>oino%/i{n/EZ?~}y8qPG|[+!;<uLQgO?tW;/pv6OmUwXoxk[K5/s!}vv"GPcD4?zzL8g_Ohp3KGmy(Ik]WOD <__'}C_m69%z~}r5~91] X<K#m;}E;8|9*+p]}onumQX)7ttDuOKhWB=XPW0?y@~GmP=9]L-]wqM^^>~7CId=i]SFQy1wU8#tnw!9|>?G'@On_4p>g
Feb 3, 2021 19:50:18.633610010 CET	2325	OUT	GET /css/plugins/alerts.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:18.799770117 CET	2331	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:16 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:56:04 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:16 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 1915 Keep-Alive: timeout=20, max=298 Connection: Keep-Alive Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 5a ed 8f d3 36 18 ff 7e 7f 45 06 42 bb 93 2e 51 92 26 7d 3b 21 71 70 20 21 0d 6d 12 48 43 9a f6 c1 4d 9c d6 ba 36 ae 12 97 eb 31 f1 bf cf 8e e3 c4 8e ed 24 85 03 b4 41 8b b8 d6 7d f2 bc fc 9e 57 3b f1 ca 3b 08 89 8b 3f c0 62 0b ee 9d 7f ce 1c fa 5a 81 e4 76 5d e0 43 9e ba 09 de e2 62 e9 3c 7e f5 ea d5 55 f5 9b bb 2b dd 0c 6d 09 a4 ab 8f f6 05 5e a3 74 79 f3 fe f5 0e ac e1 bb 02 e4 65 86 8b 9d f7 06 25 05 2e 71 46 bc eb ed 7e 03 ce 7f df 83 04 91 fb a7 91 7f f1 e8 ca 22 a2 58 af c0 79 18 c7 97 4e fb 9f ef 2d 2e 38 fd 1e 97 88 20 9c 2f 9d 0c 1d 61 ca 17 b7 30 23 4b c7 e7 5f 0a b4 de b4 df 08 de 37 9f 57 98 10 bc 6b be a6 a8 dc 53 5b 97 4e 8e 73 c8 97 3e ba 28 4f e1 71 e9 04 3e 7d 5d 9d 7d 3a 3b f3 38 30 60 0b 0b 62 87 25 cb 32 21 e3 e8 96 1b 90 e2 3b 2a 87 be 27 fe fe e8 3c 4e 52 f6 e6 14 77 28 25 9b a5 13 cd e6 fb 63 ad 23 3c 32 01 68 4d ad 4a 60 4e 21 1d b4 35 f6 9f 48 f6 35 df 76 a0 58 a3 dc e5 34 6e 18 4f 85 88 fa 87 8a da 0d 7d 5f ac 33 7f 67 5b a6 ec 06 a5 29 cc 87 91 59 b0 57 ad 1f 48 53 94 af 5d 81 6b 58 b1 a5 98 3d db c1 14 01 07 6c b7 0e c8 53 e7 7c 07 8e 6e 6d 76 1c 51 a2 8b 1a 48 03 b6 12 42 e0 40 f0 55 b3 a8 98 e6 6b eb aa d7 5b a0 82 58 98 2a c5 46 bb f8 49 73 f1 26 ac 35 11 ae 8d 67 ec cd c9 33 9c 13 b7 44 1f a1 30 b6 eb 3e 26 54 22 bd 83 5c e0 c4 f7 25 5a 22 f2 43 06 b8 75 76 01 b7 80 a0 0f 50 f6 1c 0f a6 80 05 93 af 80 bf ac 16 eb d0 40 39 74 37 b5 c8 30 14 cb 8d 37 57 5b 9c dc ea 41 bd ef 1a 1c c7 fd 2a c9 06 a3 7c 03 0b 44 3a 3a b5 e0 d0 e0 02 44 b6 b3 b1 47 57 64 75 a0 71 94 db 93 ec e6 66 fa 5c e8 66 48 bc 22 65 b5 a8 95 24 a7 62 bb 2a b9 30 98 35 5a ca ce 0a 85 b3 e8 ca ea 16 11 97 b3 76 0b 90 a2 43 49 9d 29 ae b2 ad 2b ae 91 b0 48 0e 45 c9 94 de 63 c4 93 dc 0c c0 32 c3 c9 a1 ac 61 c0 07 c2 dc 2a d5 30 b5 be 50 2f f3 8a 19 84 f3 4b 6a d1 82 56 cc 49 55 31 e3 8b 4b ea 9d 12 92 8a 8e 06 8f a0 f4 e9 af fc 9f e7 c7 17 dd 28 0b 44 12 9b 34 db b0 7a 61 77 10 08 d2 45 16 5a af 06 09 8b 21 fb e5 f3 20 49 20 b4 5d ee 25 20 4f e0 d6 7e 39 f4 d9 5b 0d 8f c9 64 a2 f3 f3 4a e0 a2 a4 89 b4 ba dc cc 1b 3f 89 14 6a 57 44 70 45 14 c3 12 6f 51 ea ac 0b 70 df 1b 25 91 6f 09 93 4e b1 e6 c9 22 15 bb 26 7a fc fe 2c ac 22 01 7d ac 48 a9 31 84 36 0e aa 83 c1 77 c2 5c f6 17 16 05 6e 1c c8 f5 6a 3a 7b 38 8b 66 d1 98 cb d9 a7 a3 4b d5 bf ad 39 d9 54 1c aa 3c 66 d6 2c de 35 c6 60 45 71 3f 10 a8 7a a8 a9 e3 4d 53 6d 40 37 8c 2e b5 Data Ascii: Z6~EB.Q&};!qp !mHCM61$A}W;;?bZv]Cb<~U+m^tye%.qF~"XyN-.8 /a0#K_7WkS[Ns>(Oq>}]};;80`b%2!;* '<NRw(%c#<2hMJ`N!5H5vX4nO}_3g[)YWHS]kX=lS|nmvQHB@Uk[X*FIs&5g3D0>&T"\%Z"CuvP@9t707W[A*|D::D GWduqf\fH"e$b*05ZvCI)+HEc2a*0P/KjVIU1K(D4zawEZ! I]% O~9[dJ?jWDpEoQp%oN"&z,"}H16w\nj:{8fK9T<f,5`Eq?z MSm@7.
Feb 3, 2021 19:50:19.431134939 CET	2357	OUT	GET /css/fonts/fontawesome.woff2?v=4.6.3 HTTP/1.1 Host: eriglobal.com Connection: keep-alive Origin: http://eriglobal.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://eriglobal.com/css/default.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.597676039 CET	2443	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:51:40 GMT Accept-Ranges: bytes Content-Length: 71896 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=297 Connection: Keep-Alive Content-Type: font/woff2 Data Raw: 77 4f 46 32 00 01 00 00 00 01 18 d8 00 0e 00 00 00 02 54 c8 00 01 18 79 00 04 01 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 46 46 54 4d 1c 1a 20 06 60 00 86 02 11 08 0a 88 bb 50 86 e9 4b 01 36 02 24 03 95 00 0b 95 18 00 04 20 05 86 7c 07 b2 4c 3f 77 65 62 66 06 5b 38 e0 91 00 d6 6d 3b af 74 05 e9 cd fa d3 d5 e7 e8 00 63 36 c2 d6 9b 15 96 f0 3e bc 53 ad 38 ae 7b 1c 80 19 5d 3f fb ff ff 3f 3d 69 8c a1 25 81 e6 00 50 d5 da ae da ad fb ff cf 66 38 35 4a 88 30 aa b9 75 04 0f b2 98 66 b1 b0 c9 65 42 af 5c d8 eb a6 02 45 b9 6c fb fd e8 fd 81 41 77 98 d6 36 84 11 1c 66 b3 11 46 c0 8e a0 30 6c 9b 0d c3 b6 4d 81 60 3b 69 96 4f df 9e 55 13 cb d4 b1 e6 6b d9 b6 22 3d e8 cb b2 0b eb c3 ba 8a 96 f2 90 c1 2f 36 0f e1 2f 65 58 0d 71 a4 d5 76 66 7b 5d f2 2d 03 6f 2c e9 35 cb 26 bf 7d 9a 4c e6 cb 3a 9c 1a c6 30 1e 7b f0 65 fe c6 a5 56 2a 33 7e a6 82 8a ca 31 4d 68 1d 4d 34 3a 39 6a 47 15 ef 42 13 0f ab 8a 15 e6 4b af b7 f7 59 e8 97 db 32 63 11 3d b9 de 40 c7 0f 56 2a 2b 9e cb 3d ed a3 67 b9 3b df 9f f5 25 ca 71 2c 7f af 73 59 46 ba 6f 6a df f3 44 fe 7f 74 f2 f6 7f df 77 5a 31 74 c3 53 5c 91 af a4 4c e2 8d 87 fe a4 f7 dc 6b 28 e3 f6 02 31 43 4b e7 7a 9f 5a 21 e0 69 4d 7f 9e ee 1e 7a 48 8c d8 86 92 e6 ea 44 5b 67 63 4e 9c a4 c2 d5 a9 13 a9 c5 f6 45 db 7e 05 6a c2 56 44 f9 0d 5b 15 d2 2f 9e 8b 54 44 c8 fa a1 cb be e6 7f 15 a8 10 05 3c 40 c2 6a 19 63 6c cb b4 bb db 7d 9c 73 dd 67 34 13 84 d7 46 e9 66 93 46 9b c4 3b 04 db ec 48 83 0a 01 45 10 11 b0 50 01 23 49 15 bb 31 7b f6 1c 58 b1 cd 9c d3 b9 e9 aa 5d b5 cb 70 73 91 ba 88 fe 9f eb d2 fe 93 5e 28 a9 53 b6 9d 2e ab bd 9d 91 03 4e c2 8f 03 ac 31 53 fe f0 df 9c fd cf 24 40 db 99 a4 54 02 5c d3 d5 6b 22 47 22 15 20 56 13 5a 12 e6 67 66 3f 93 7b ff 8e 44 a0 9a 38 66 81 aa ec fa 91 ed f6 c9 15 93 9f 9e 39 fb 9f b9 cf 67 e0 69 12 5c ab 88 d6 e5 ee 8e 20 db 22 d9 96 75 5e 1f 2b 84 f9 89 fc 25 e4 f9 d7 75 af 53 aa 8a cf 99 21 e1 4a 04 59 35 9a 7b 6b fa a5 6a b5 a9 4a b2 9d cc 12 f3 69 a0 c1 f0 c9 21 7f 84 74 eb 22 bd bd a9 76 d9 10 fa 43 94 0c 30 1b 96 e1 70 9a 97 61 73 96 9c 67 0a 33 b3 7f be ff a9 7e 33 2f 8b 33 bb 3c 73 af c0 b1 0b 02 4b b2 9d b4 75 08 8b 74 af 6e 12 97 1c 17 1e e5 e5 74 53 b0 7c 7f a4 5d 96 7e 81 0c 49 2a 20 db 01 03 49 b2 03 0e a0 e3 01 37 79 b0 e1 45 4c 40 f0 96 42 15 25 13 92 fd df 54 54 54 f5 7a 75 5c 99 dd df 18 eb 65 62 a4 62 4d 0b 2e 2d 66 f4 3f d9 fb f8 00 20 08 4f 73 24 2f 2e 59 a3 1d a0 b9 75 0b a2 37 18 03 46 8d 51 35 d8 46 0d d8 ad 8a 15 db e8 8d dc 88 1c d1 1b 25 a5 b4 0a a2 02 a2 a2 62 60 a3 18 d8 6f d5 ab ff 06 da 6f d4 fb ad 8f 63 1c 80 0e 74 03 dd Data Ascii: wOF2Ty?FFTM `PK6$ |L?webf[8m;tc6>S8{]??=i%Pf85J0ufeB\ElAw6fF0lM`;iOUk"=/6/eXqvf{]-o,5&}L :0{eV*3~1MhM4:9jGBKY2c=@V*+=g;%q,sYFojDtwZ1tS\Lk(1CKzZ!iMzHD[gcNE~jVD[/TD<@jcl}sg4FfF;HEP#I1{X]ps^(S .N1S$@T\k"G" VZgf?{D8f9gi\ "u^+%uS!JY5{kjJi!t"vC0pasg3~3/3<sKutntS\|]~I* I7yEL@B%TTTzu\ebbM.-f? Os$/. Yu7FQ5F%b`ooct
Feb 3, 2021 19:50:20.119328022 CET	2785	OUT	GET /css/fonts/opensans-semibold.woff HTTP/1.1 Host: eriglobal.com Connection: keep-alive Origin: http://eriglobal.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://eriglobal.com/css/default.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.285129070 CET	2940	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:54:51 GMT Accept-Ranges: bytes Content-Length: 24964 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=296 Connection: Keep-Alive Content-Type: application/x-font-woff Data Raw: 77 4f 46 46 00 01 00 00 00 00 61 84 00 13 00 00 00 00 b0 bc 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 68 61 33 bd 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 17 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a2 00 00 09 98 2c 1a 16 58 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 5e 88 92 4f 53 2f 32 00 00 07 0c 00 00 00 5f 00 00 00 60 a1 cc 92 8e 63 6d 61 70 00 00 07 6c 00 00 01 86 00 00 01 da cf 40 58 a0 63 76 74 20 00 00 08 f4 00 00 00 3a 00 00 00 3a 13 db 0d fe 66 70 67 6d 00 00 09 30 00 00 01 b1 00 00 02 65 53 b4 2f a7 67 61 73 70 00 00 0a e4 00 00 00 0c 00 00 00 0c 00 08 00 1b 67 6c 79 66 00 00 0a f0 00 00 4d 52 00 00 91 3c cf 59 90 86 68 65 61 64 00 00 58 44 00 00 00 34 00 00 00 36 0b f3 b0 fe 68 68 65 61 00 00 58 78 00 00 00 1f 00 00 00 24 0f 79 06 27 68 6d 74 78 00 00 58 98 00 00 02 3a 00 00 03 a6 f5 1a 52 23 6c 6f 63 61 00 00 5a d4 00 00 01 cb 00 00 01 d6 8a c4 68 26 6d 61 78 70 00 00 5c a0 00 00 00 20 00 00 00 20 02 07 01 9a 6e 61 6d 65 00 00 5c c0 00 00 02 21 00 00 04 f6 64 4c b0 b7 70 6f 73 74 00 00 5e e4 00 00 01 ed 00 00 02 e5 1a 78 32 a8 70 72 65 70 00 00 60 d4 00 00 00 a5 00 00 00 f6 7f df 42 f7 77 65 62 66 00 00 61 7c 00 00 00 06 00 00 00 06 f5 f2 56 b0 00 00 00 01 00 00 00 00 cc 3d a2 cf 00 00 00 00 c9 4c ea 7d 00 00 00 00 d2 d6 a6 70 78 da 63 60 64 60 60 e0 03 62 09 06 10 60 62 60 04 c2 97 40 cc 02 e6 31 00 00 0e 4d 01 1c 00 00 78 da ad 96 4b 6c 54 55 18 c7 ff 33 9d 61 c6 82 96 aa d1 f8 08 1a 32 36 b5 06 8d 0d 49 db b1 b0 6a da 5a 0d 96 69 8b 83 0e 8a 0f e2 02 42 42 63 48 4c 13 16 85 81 b8 30 21 06 2b 39 3c 6a 0a 4c a1 d0 59 90 52 9a f2 32 4c 57 2c dc e1 69 6d e3 ca e5 49 57 c4 05 21 8e bf 73 db 29 e0 48 d5 c4 7c f9 e5 dc 39 f7 bb df e3 7f ce 3d 73 15 92 54 a9 6e 7d aa 48 4b eb bb dd 7a fe b3 af 7a 77 a9 e6 8b de 1d 3b 55 bf eb 93 2f 77 6b a3 22 f8 a8 58 94 f7 fd 37 d7 a1 9d 3b 7a 77 2b ee af 02 22 0a 07 63 5c a1 78 6f e0 b9 5d b7 74 2b 74 38 34 10 ba 03 77 c3 e9 70 0e a6 c3 bf 86 73 15 ab c3 e9 8a 7d 30 16 f9 29 72 2f 72 2f 9c 8b ce af f8 2d 74 38 f6 4c ac 36 96 82 cf b9 da 0b fe 77 6d ec c7 58 2a 9e 8c 27 63 7b e3 49 e2 dd bd 6f 44 cb c1 82 a5 1f 34 e2 06 16 9d af d8 17 c4 29 59 ed c3 16 df 0e 49 4f 78 3a 3a 4f a5 77 82 aa 07 02 de 54 a2 b8 47 0d 7a 55 4d 90 84 66 3d ad 96 62 5e ad c5 ac da a0 1d 3a 8a 05 75 c2 66 48 f1 bb 8b b1 9b b1 87 71 0b a4 a1 9f 38 fb e1 00 64 e1 20 1c 82 41 e2 0d e1 7b 8a 98 a7 e1 0c e4 60 18 ce c2 39 ee 8d c0 79 b8 00 a3 30 06 97 60 1c 2e c3 04 4c c2 15 f2 5c 85 6b Data Ascii: wOFFaFFTMha3GDEF GPOS,XGSUB^OS/2_`cmapl@Xcvt ::fpgm0eS/gaspglyfMR<YheadXD46hhe aXx$y'hmtxX:R#locaZh&maxp\ name\!dLpost^x2prep`Bwebfa|V=L}pxc`d``b`b`@1MxKlTU3a26IjZiBBcHL0!+9<jLYR 2LW,imIW!s)H|9=sTn}HKzzw;U/wk"X7;zw+"c\xo]t+t84wps}0)r/r/-t8L6wmX*'c{IoD4)YIOx::OwTGzUMf=b^:ufHq8d A {`9y0`.L\k
Feb 3, 2021 19:50:20.296612024 CET	2987	OUT	GET /uploads/videos/c4ca4238a0b923820dcc509a6f75849b/videoplayback-1558705888.mp4 HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: identity;q=1, *;q=0 Accept: */* Referer: http://eriglobal.com/ Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english Range: bytes=0-

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.464545012 CET	3170	IN	HTTP/1.1 206 Partial Content Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Fri, 24 May 2019 13:51:28 GMT Accept-Ranges: bytes Content-Length: 16811173 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Range: bytes 0-16811172/16811173 Keep-Alive: timeout=20, max=295 Connection: Keep-Alive Content-Type: video/mp4 Data Raw: 00 00 00 18 66 74 79 70 6d 70 34 32 00 00 00 00 69 73 6f 6d 6d 70 34 32 00 00 76 dc 6d 6f 6f 76 00 00 00 6c 6d 76 68 64 00 00 00 00 d8 de 80 d1 d8 de 80 d1 00 00 03 e8 00 00 f5 14 00 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 47 7b 74 72 61 6b 00 00 00 5c 74 6b 68 64 00 00 00 03 d8 de 80 d1 d8 de 80 d1 00 00 00 01 00 00 00 00 00 f5 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 05 00 00 00 02 d0 00 00 00 00 00 24 65 64 74 73 00 00 00 1c 65 6c 73 74 00 00 00 00 00 00 00 01 00 00 f5 09 00 00 03 e9 00 01 00 00 00 00 46 f3 6d 64 69 61 00 00 00 20 6d 64 68 64 00 00 00 00 d8 de 80 d1 d8 de 80 d1 00 00 75 30 00 1c b7 18 55 c4 00 00 00 00 00 5f 68 64 6c 72 00 00 00 00 00 00 00 00 76 69 64 65 00 00 00 00 00 00 00 00 00 00 00 00 49 53 4f 20 4d 65 64 69 61 20 66 69 6c 65 20 70 72 6f 64 75 63 65 64 20 62 79 20 47 6f 6f 67 6c 65 20 49 6e 63 2e 20 43 72 65 61 74 65 64 20 6f 6e 3a 20 30 34 2f 31 38 2f 32 30 31 39 2e 00 00 00 46 6c 6d 69 6e 66 00 00 00 24 64 69 6e 66 00 00 00 1c 64 72 65 66 00 00 00 00 00 00 00 01 00 00 00 0c 75 72 6c 20 00 00 00 01 00 00 46 2c 73 74 62 6c 00 00 00 98 73 74 73 64 00 00 00 00 00 00 00 01 00 00 00 88 61 76 63 31 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 02 d0 00 48 00 00 00 48 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 ff ff 00 00 00 32 61 76 63 43 01 64 00 1f ff e1 00 1b 67 64 00 1f ac d1 00 50 05 bb 01 6a 02 02 02 80 00 01 f4 80 00 75 30 07 8c 18 89 01 00 04 68 eb 8f 2c 00 00 00 18 73 74 74 73 00 00 00 00 00 00 00 01 00 00 07 58 00 00 03 e9 00 00 00 58 73 74 73 63 00 00 00 00 00 00 00 06 00 00 00 01 00 00 00 0e 00 00 00 01 00 00 00 42 00 00 00 0d 00 00 00 01 00 00 00 45 00 00 00 0e 00 00 00 01 00 00 00 67 00 00 00 0d 00 00 00 01 00 00 00 6a 00 00 00 0e 00 00 00 01 00 00 00 87 00 00 00 0a 00 00 00 01 00 00 02 2c 73 74 63 6f 00 00 00 00 00 00 00 87 0 0 00 76 fc 00 04 f1 c3 00 06 06 79 00 06 e2 82 00 07 d2 d3 00 0a f9 a7 00 0c bc 5a 00 0e 66 2e 00 0f b4 78 00 14 09 15 0 0 15 90 dd 00 16 d0 c1 00 18 12 72 00 1b bb 21 00 1d 37 Data Ascii: ftypmp42isommp42vmoovlmvhd@G{trak\tkhd@$edtselstFmdia mdhdu0U_hdlrvideISO Media file produced by Google Inc. Created on: 04/18/2019.Flminf$dinfdrefurl F,stblstsdavc1HH2avcCdgdPju0h,sttsXXstscBEgj,stcovyZf.xr!7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49774	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:17.212126970 CET	2172	OUT	GET /js/default.js HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:17.381728888 CET	2187	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:14 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 04 Mar 2019 19:50:26 GMT Accept-Ranges: bytes Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:14 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=300 Transfer-Encoding: chunked Content-Type: application/javascript; charset=utf-8 Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 dc fd 69 77 db 56 96 30 0a 7f ef b5 fa 3f 90 a8 b4 04 98 87 14 65 27 d5 15 d0 10 5f c7 76 2a 4e ec d8 15 3b 95 54 51 8c 1b 13 49 48 24 41 93 94 25 45 64 ff f6 77 0f 67 04 40 d9 a9 ee e7 de 67 dd aa 58 04 0e ce 3c ec b3 e7 7d f2 a0 dd ba f8 5b eb e3 69 ef f4 b4 f7 a8 f5 e0 e4 df ff ad 3d b9 5a a6 db a2 5c fa b1 48 82 3b af 4c 2e f2 74 eb 45 d1 f6 76 95 97 93 d6 a2 cc ae e6 f9 d1 d1 81 0f bd fc 66 55 ae b7 9b a1 fb 1a c5 bd ac 4c af 16 f9 72 3b 4c a0 e6 76 3f 08 4d 43 c1 5d 31 f1 db 26 4b b0 9d ad cb eb d6 32 bf 6e 3d 5f af cb b5 ef 5d fc ed 2a 5f df b6 d6 f9 87 ab 62 9d 6f 5a 71 eb ba 58 66 90 e7 ba d8 ce e0 4d 95 f4 82 c1 3a df 5e ad 97 2d 68 25 d8 87 f4 d7 f7 ae 96 59 3e 29 96 79 e6 b5 55 77 b9 fc 90 7f c2 ed ac d8 08 77 e4 1f e3 75 2b 8d 46 63 91 45 69 6f 33 2f d2 5c e4 f0 94 96 cb 34 de 8a 09 3c ae ae 36 33 31 85 07 a8 23 bf 79 3d 11 b3 e8 6e 2f 8a 68 d6 db 96 6f b7 eb 62 39 15 17 f0 32 8b 37 af af 97 6f d6 e5 2a 5f 6f 6f c5 25 66 9a 47 1e cf b9 27 16 91 db ae ec 3f 0e 7e d1 9b 2c a1 f2 62 4b 5f f6 62 19 9d fc 36 3a df 9c 5f 7d fb fc db 6f cf 6f 9e f4 c7 9d 5d e5 fd 8b 93 a9 28 21 5b 77 b1 e9 9e 88 55 74 d2 f5 47 e7 59 dc fd 7d 1c 9c 4c 0b f1 a1 b9 b1 04 7a fc f3 0a fa f7 34 de e4 7e b0 1f 60 cb d1 a2 b7 5a 97 db 12 27 2c ba bb f8 80 2b 10 ce 05 4c c0 66 bb be 4a b7 e5 3a 5c 88 4d 3e cf e9 d1 f3 c4 3c 5f 4e b7 b3 b0 2f b6 e5 93 f5 3a be 35 2b ac 1b ca 7a 69 3c 9f fb 38 dd 30 9e 69 be 75 76 81 1a fa d5 7c de 8e e2 61 ff 2c 1e 62 ce 51 dc c1 9f 1e d7 3f 0e 39 6d 1c ba 95 e1 6a bc dd c6 e9 a5 53 25 ae 62 02 23 59 e4 eb 69 4e 59 7b d6 00 fc 40 c4 66 c7 c0 70 f3 8f af 69 5b 47 b4 21 12 cc bb cd 6f f8 55 bd 88 64 2f f2 38 9d 85 8d 53 b9 e8 e1 37 6a 49 f0 aa 2d e2 55 d3 28 a9 4a dd 69 1f ba 18 af 7c 77 1f 26 22 d5 d9 63 1e 2c 24 61 a5 01 d4 4b 7b b2 61 8e 2b 15 67 bd 78 b5 9a df ca 1e ad a7 74 4e 36 58 c1 a4 58 6f b6 87 2a c8 3f f8 7d c8 33 8f ef cd d2 3d 85 3c f9 87 86 29 b7 56 4c a4 51 27 ee f8 b8 9c 49 d8 d7 f3 5d e9 67 7a 16 f5 8f 8e 92 b3 74 38 a2 05 4e c7 e3 70 34 c6 ea 97 d9 c1 51 ea 05 db ed 6a 6b 8b db 48 ee 8b 70 22 36 00 86 42 38 c8 f0 23 36 2b 9a 3a 78 a3 07 58 22 80 53 5b 68 27 a2 13 27 9f ad 36 71 48 b0 98 30 f7 99 c8 c5 04 0e bd 9e c8 51 7f bc db c1 89 9e 45 a7 70 Data Ascii: 1faaiwV0?e'_v*N;TQIH$A%Edwg@gX<}[i=Z\H;L.tEvfULr;Lv?MC]1&K2n=_]*_boZqXfM:^-h%Y>)yUwwu+Fc Eio3/\4<631#y=n/hob927o*_oo%fG'?~,bK_b6:_}oo](![wUtGY}Lz4~`Z',+LfJ:\M><_N/:5+zi<80iuv|a,bQ?9mjS%b#Yi NY{@fpi[G!oUd/8S7jI-U(Ji\|w&"c,$aK{a+gxtN6XXo*?}3=<)VLQ'I]gzt8Np4QjkHp"6B8#6+:xX"S[h"6qH0QEp
Feb 3, 2021 19:50:18.633806944 CET	2326	OUT	GET /css/plugins/box.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:18.797029018 CET	2328	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:16 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:56:04 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:16 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 938 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 03 dd 56 5f 6f db 36 10 7f f7 a7 e0 6c 14 48 8a 48 51 12 bb 4d 14 14 28 16 6c c3 80 74 1d b6 16 7b a6 48 4a 22 42 e9 04 8a 8a 9d 14 05 fa b8 7d ce 7d 91 1e 29 ca 92 22 25 41 81 3e 35 0e 6c 91 ba e3 dd fd 7e f7 87 6f 59 4e 75 2d 0c 59 7e fc f0 6b 70 be bc 5c ac 18 28 d0 09 ec 8e c8 8a e1 cf fb 5b a1 15 bd f3 ab 7f 34 ad 2a a1 c9 a7 05 21 15 d4 d2 48 28 63 42 93 1a 54 63 c4 25 ee 1a a8 62 12 d9 27 25 52 e3 1f ef 03 59 72 b1 8b c9 05 fe 91 9f 64 51 81 36 b4 34 f6 1d a0 81 54 c1 36 26 b9 e4 5c 94 6e af 31 4a 96 22 26 25 94 e2 92 7c 5e 2c 86 be 3c b0 9e ca 9d e0 56 6b 2b b9 c9 63 72 12 45 2f ec 32 17 32 cb 4d bf 4e 28 bb c9 34 34 25 0f 5c 8c 31 d1 59 42 0f 4e 37 9b 23 d2 7f 45 e1 c5 61 6f f1 1d ba a4 c4 35 46 e2 01 f8 19 8c 81 c2 6e 38 2f 98 12 14 0f b2 a1 f6 4a 57 50 1a 51 9a 07 6e 6a a1 a8 91 b7 83 70 ae 81 72 c1 87 d2 3d 16 b4 31 60 25 09 99 11 cd 5b 02 08 29 a8 ce 64 69 43 ac 76 24 38 c3 ef f1 e9 b2 cc c6 fc f9 cd df 90 c6 5c b2 6f a5 f1 29 80 f7 76 ff d4 e2 56 42 53 7b 8b 7f 88 5d 87 dd 95 82 5a f8 e7 bf 95 e4 a2 ce 61 db c2 d8 e8 da 12 52 81 c4 08 b5 3b 2c 74 87 e5 60 c0 89 20 2c d4 78 a4 17 7d e4 0e 27 4b 2e 68 2e b4 f7 93 cb ba c2 98 63 92 28 60 37 ad f8 2e f0 de ef 53 ca 19 f8 3d d5 b4 10 ce c2 33 e9 33 3d b4 b7 d9 06 3f 2e 1c 4f d6 d1 1c 81 9f 9c f6 2e a8 e5 3d b2 11 13 d6 ee 07 b8 67 0f 0e 0a b8 0f 9e 7a bf 15 c9 8d 34 8f 8a cc 66 62 9f fe 31 59 a5 69 3a 5b 7b 73 b8 4c 14 f7 c7 ff a2 35 f8 5e 40 39 77 6e 6c 6c 0e 0e b0 39 c1 c4 c4 ac 92 1c 61 60 ac 57 fd 20 8d ea 72 e1 aa d1 ba f3 72 8f f2 b8 f2 c7 e9 32 9f b2 89 2b 4d a4 a3 f5 40 b7 f4 ad 4f db a5 2f f9 d5 7a bd 9e e6 ea 8c e9 47 cd 40 45 99 34 77 3e d5 5c 9d ac 2f 5e f4 95 12 ac a3 a9 45 9b c0 c8 85 65 0b bb da b9 97 a8 2b 41 6f 7a 7b 4e 62 eb d3 ee 2c 8a 86 54 b7 da 05 80 c9 1d ce d8 3c 25 55 92 d6 6d eb 1b 72 d4 1d 37 2a 09 83 65 18 d4 39 e5 96 ec 08 3f 96 18 cb e6 51 bb b2 0d 64 85 cd 79 d0 73 3a 70 e2 dc a6 89 ef 38 fb e8 4f e6 24 53 60 1e cc 41 0f 8f e6 24 13 91 82 16 5e d4 e7 6e 4c 96 ff 7f f9 77 d9 d3 63 7b c7 f7 a1 c6 27 c3 0f c3 8d 45 e6 79 5e 9c d4 b3 9c 38 a9 47 f9 f8 6f f9 d8 48 79 6e 7a 9c 6d 06 55 b1 7e 38 83 db 5e 42 1a ad 0e c2 f0 18 ff 65 41 33 51 1f 27 32 0b 54 6b 27 cc 64 7a 88 90 05 5a 20 19 86 6c 10 87 cd 70 c4 b9 81 f2 84 1b 9e f5 53 4f a9 f3 aa 5b f8 6e df 2d bb 6e df ad fb 54 0a 5f 4d 08 1b 46 31 09 a0 a9 9c fb e9 5d c0 68 c9 84 0a ab 32 1b 46 c1 84 Data Ascii: V_o6lHHQM(lt{HJ"B}})"%A>5l~oYNu-Y~kp\([4*!H(cBTc%b'%RYrdQ64T6&\n1J"&%|^,<Vk+crE/22MN(44% \1YBN7#Eao5Fn8/JWPQnjpr=1`%[)diCv$8\o)vVBS{]ZaR;,t` ,x}'K.h.c(`7.S=33=?.O.=gz4fb1Yi:[{sL5^@9wnll9a`W rr2+M@O/zG@E4w>\/^Ee+Aoz{Nb,T<%Umr7*e9?Qdys:p8O$S`A$^nLwc{'Ey^8GoHynzmU~8^BeA3Q'2Tk'dzZ lpSO[n-nT_MF1]h2F
Feb 3, 2021 19:50:19.426593065 CET	2356	OUT	GET /css/fonts/oswald-light.woff2 HTTP/1.1 Host: eriglobal.com Connection: keep-alive Origin: http://eriglobal.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://eriglobal.com/css/default.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.589679003 CET	2415	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:55:36 GMT Accept-Ranges: bytes Content-Length: 19548 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=298 Connection: Keep-Alive Content-Type: font/woff2 Data Raw: 77 4f 46 32 00 01 00 00 00 00 4c 5c 00 12 00 00 00 00 ae c4 00 00 4b f7 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 46 46 54 4d 1c 1a 28 1b 94 72 1c 24 06 56 00 86 6e 08 2e 09 92 62 11 08 0a 82 8a 74 81 f1 4d 01 36 02 24 03 8d 04 0b 86 44 00 04 20 05 89 78 07 20 0c 81 05 1b 9d 9d 17 70 de 96 e4 dc ed 40 10 bb dc 5f ac 60 1c 5b 01 99 07 08 0d e4 d7 66 47 68 8f 83 92 b8 96 d9 ff ff e7 24 1d 63 38 66 0d 14 d5 ec ef 1d 62 1e 4e dd e1 aa 4d 35 32 b3 b5 3e d0 e7 ea 69 9a 5b 47 e6 a8 97 d0 f6 42 c8 64 cf bb 27 02 55 48 84 23 3a fb c8 a9 44 e5 cc d1 88 bb f3 f9 95 86 15 a6 48 e0 2b 59 e1 a6 e1 61 ee a2 ab 68 d8 89 be ab 55 97 79 cc ce 83 06 ae 9b 8e c2 65 e6 cf c8 be dc ad ac 78 2a 20 be 0b f7 29 1a db 67 f9 1f d2 4f f2 62 41 65 eb f5 90 8c 20 2b a8 48 b2 2a 7f d6 be a0 0e e7 3f b1 ac ce d6 e3 2c 9b d3 57 6c 62 e1 4e bb e0 ec 2d 11 13 44 74 60 f2 55 60 ec f2 18 51 2b 4e fb fa ff af d3 ba ef bd 0f 22 cb 96 0c b1 c7 8e a3 d8 89 03 8a 1d a4 3f 00 a0 05 c2 8a b8 dd b3 f5 6e 35 35 f7 53 2e b5 3b 40 db ec 48 01 b1 50 01 13 c5 c0 46 01 05 63 48 8b 52 92 16 60 61 31 63 8a 81 8d b3 e6 9c 73 16 ba 74 9b 2e ca df d4 05 db 7e ba ea df fa 7b ef ea 57 f1 51 7b a8 6a 98 f6 cc ec 95 a0 70 a4 8f 05 53 76 a2 11 3a 23 2e e6 00 b0 a9 29 32 32 c0 ae df e5 e1 f9 75 7c e7 ce 7c 70 c9 59 80 09 8c ce eb 04 b6 2d 59 6e 80 22 d9 40 be e3 e7 f6 8d 94 88 99 4c 68 34 1a a1 91 68 96 bc 8a 3f d4 be ca ec 76 98 ce f4 b2 cd 7f 08 81 0a 95 6c 04 af c4 d0 36 5f 6d 67 fe d1 0f a7 fb 93 f6 00 79 c0 cb ff 23 7b b6 f3 36 f8 3d 52 02 85 44 32 44 37 2d 36 66 c8 5a a2 b9 f8 2f 91 9c 5e 20 98 d6 a1 fd 7b 6d e6 cf 2c da 33 92 37 40 45 9b 32 57 d5 e7 33 ac cf 0e 00 48 3b 8d 64 07 77 cf 5d 2a a2 a2 a4 96 c9 be 00 7d 2e ff eb f3 7f 75 1a 61 85 80 98 f8 47 ee 6e 34 a9 74 ed eb f9 06 1d e5 d4 66 ed 24 6d b5 d1 21 e3 ae 64 28 10 eb e3 e6 38 4c 06 c6 10 0b 0a af c3 f7 3d 1b ff 10 72 cd 6d 53 89 41 e5 d3 ef b5 00 f0 bf 5f da e7 39 e7 de fb de eb a8 b0 21 04 6d 4a f6 cc b6 34 0e 49 96 5b 3f 68 da 09 a9 ba 66 d0 2e 36 4b d0 04 bb f8 40 27 80 6d 40 cc 0d c8 f2 ff bf ba 76 c0 b4 fc d7 09 8b d2 fa 84 f9 76 e6 49 ea a9 a8 ff af ee 35 29 f0 06 a4 c2 55 5f 81 ec 02 05 54 7a ff f3 94 b0 54 94 6c e7 cf 5d c6 1e 6d d3 95 cb be ba d7 ec 8e b1 d0 97 2c a7 23 8f b7 fc d5 04 1c 4b 4e 2a e2 b7 01 a4 07 a1 aa f9 e5 20 51 26 55 ec 57 5a af 63 86 31 cb 16 e4 ff 4c d5 da 19 80 90 17 92 78 8f 74 a4 9d a9 4b 94 53 e8 4d e7 dc 5f d3 0c fe ec 62 67 36 00 c4 2e 09 2f 17 24 05 01 12 4d 82 b2 44 00 4a 84 13 b1 00 f8 00 06 3d da 99 d2 45 56 8e 51 be 40 52 89 76 a6 e8 94 2e c6 d0 d4 57 f9 Data Ascii: wOF2L\K?FFTM(r$Vn.btM6$D x p@_`[fGh$c8fbNM52>i[GBd'UH#:DH+YahUyex* )gObAe +H*?,WlbN-Dt`U `Q+N"?n55S.;@HPFcHR`a1cst.~{WQ{jpSv:#.)22u\|pY-Yn"@Lh4h?vl6_mgy#{6=RD2D7-6fZ/^ {m,37@E2W3H;dw]*}.uaG n4tf$m!d(8L=rmSA_9!mJ4I[?hf.6K@'m@vvI5)U_TzTl]m,#KN* Q&UWZc1LxtKSM_bg6./$MDJ=EVQ@Rv.W
Feb 3, 2021 19:50:19.821652889 CET	2545	OUT	GET /images/cuild2.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.984842062 CET	2660	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:29 GMT Accept-Ranges: bytes Content-Length: 25396 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=297 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 39 45 38 32 37 45 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 38 42 41 30 33 32 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:249E827E33B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:248BA03233B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:
Feb 3, 2021 19:50:20.153239012 CET	2807	OUT	GET /images/build3.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.316802979 CET	2992	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:17 GMT Accept-Ranges: bytes Content-Length: 15822 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=296 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 39 45 38 32 38 32 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 39 45 38 32 38 31 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:249E828233B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:249E828133B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:
Feb 3, 2021 19:50:20.346245050 CET	3077	OUT	GET /images/bottom-BG2.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/css/custom.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.511528015 CET	3274	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Wed, 06 May 2020 14:53:38 GMT Accept-Ranges: bytes Content-Length: 305149 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=295 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 20 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 35 36 30 44 39 45 37 41 38 37 43 44 31 31 45 41 42 37 35 46 39 38 30 41 41 44 41 33 44 30 46 43 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 36 30 44 39 45 37 39 38 37 43 44 31 31 45 41 42 37 35 46 39 38 30 41 41 44 41 33 44 30 46 43 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 61 33 65 63 37 37 61 31 2d 65 61 33 66 2d 34 62 31 62 2d 38 61 63 62 2d 32 35 38 35 38 61 39 39 63 62 34 64 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:560D9E7A87CD11EAB75F980AADA3D0FC" xmpMM:InstanceID="xmp.iid:560D9E7987CD11EAB75F980AADA3D0FC" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:a3ec77a1-ea3f-4b1b-8acb-25858a99cb4d" stRef:documentID="adobe:docid:photoshop
Feb 3, 2021 19:50:21.534107924 CET	4503	OUT	GET /images/ico/favicon.png HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english; _ga=GA1.2.406443051.1612410619; _gid=GA1.2.696941932.1612410619

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:21.698930025 CET	4504	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:19 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:51 GMT Accept-Ranges: bytes Content-Length: 1823 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:19 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=294 Connection: Keep-Alive Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f f3 ff 61 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 24 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 53 36 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 41 34 38 45 41 46 43 39 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 41 34 38 45 41 46 43 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 38 36 33 43 36 35 39 32 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 41 34 38 45 41 46 43 38 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d 70 6d 65 74 Data Ascii: PNGIHDRatEXtSoftwareAdobe ImageReadyqe<$iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0 MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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 CS6 (Macintosh)" xmpMM:InstanceID="xmp.iid:A48EAFC960D711E38635AE94CD148911" xmpMM:DocumentID="xmp.did:A48EAFCA60D711E3 8635AE94CD148911"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:863C659260D711E38635AE94CD148911" st Ref:documentID="xmp.did:A48EAFC860D711E38635AE94CD148911"/> </rdf:Description> </rdf:RDF> </x:xmpmet

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49775	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.159769058 CET	2333	OUT	GET /css/custom.css HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.323069096 CET	2339	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:16 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Fri, 19 Apr 2019 13:38:00 GMT Accept-Ranges: bytes Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:16 GMT Vary: Accept-Encoding Content-Encoding: gzip Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Length: 2136 Keep-Alive: timeout=20, max=300 Content-Type: text/css; charset=utf-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 d5 59 eb 6e e3 36 16 fe df a7 50 c7 08 30 53 8c 34 ba d8 96 2d a3 8b 6d 8a 9d ec 00 53 74 d1 69 1f 80 92 28 9b 1d 59 14 24 39 b1 23 e8 dd f7 90 14 25 52 17 27 29 d2 dd 76 84 20 19 8a 3a f7 cb 77 c8 90 c6 97 3a a1 59 65 96 e4 11 07 ce 26 3f ef 52 92 61 f3 80 c9 fe 50 05 ee 12 16 22 9a d2 22 58 b8 0e 7b 9a bc 3e a2 62 4f 32 33 a4 55 45 8f 81 e3 e6 e7 c6 2a 53 12 e3 c2 b0 c8 11 ed 71 fd 40 e2 ea 10 38 b6 7d 63 7c 4b 8e 39 2d 2a 94 55 bb 96 e6 7a 6d e7 67 75 3d 44 d1 d7 7d 41 4f 59 6c e6 b4 24 15 a1 59 10 e1 ac 02 7a 15 cd 9b 03 46 40 5a 48 99 a0 23 49 2f c1 9b 9f cb 07 94 c6 6f 94 4f 83 53 91 be b5 ac 0f 5c 80 f2 83 f8 c8 bc bd b3 7e cf f7 ef 8c 02 e7 18 55 e6 d9 e8 e9 ee 72 14 c7 24 db 07 b6 14 cc f1 96 4c 15 78 57 d0 87 81 96 b6 ca 6a 91 b8 ec 91 86 d9 22 78 c2 9d 62 46 66 35 4d de cf a8 a2 6f de 97 28 2b cd 12 17 24 91 2c 3d bb e7 68 a0 00 4c ff b5 6e a9 da b6 bd ab f0 b9 32 63 1c d1 02 71 ab 64 34 c3 ca f6 7b 02 d6 c2 f1 0b be 38 d0 7b 30 a5 dc bf dd 4e ef 3f 38 4a 4c 2c ed a1 32 d2 f8 0a 5b 61 2c f0 38 78 d6 d6 22 88 7d 0e 04 8d f2 88 d2 54 21 6b ad f0 b1 35 59 75 49 71 40 2a 94 92 68 17 93 32 4f d1 25 08 53 1a 7d 6d 0e ee 4b 04 59 6e fd 2d 1a c8 d2 1c bc 5a 7f 3d 49 a1 e7 c2 22 be 39 2c 55 9b 3e eb 8b d5 4b 24 fd f8 f1 e3 c0 64 dc 0f e5 01 c5 f4 21 b0 0d db f0 60 95 31 6f 16 a8 a8 48 94 e2 d2 b0 20 39 aa 20 ab 0e 66 74 20 69 fc 96 c6 f1 bb ba 0d 62 19 a6 9c b3 1a a9 c0 e9 09 12 46 2e 89 04 2b 60 ea 32 0a 5c 1a f0 c7 3e 0b 7e 3f 95 15 49 2e 57 88 e0 7b 9c 3d 2d 48 e2 b3 e7 29 32 cf 14 c6 da 17 e8 72 7b 57 ab 0c 30 c2 18 72 52 7e be 14 ee b7 84 3c b7 77 6e 3d 5b 2b c4 16 a8 15 ae 28 16 19 35 45 bd 50 ab 45 5f d2 64 ee ae ec ad a6 a3 f0 7d c4 32 ac b1 e2 82 e6 ad 3f e7 19 2b 9b ac 3c 7b 3e 67 77 35 cb 38 a1 14 be d3 0c a3 e4 a7 dd 99 67 25 c2 4e 89 c7 27 a2 dc 59 cb 98 7e 90 89 dd 46 6d 55 40 59 4b 68 71 0c 22 94 f3 34 7e c4 ad 1c 06 aa 9f e2 90 e2 0a 36 9a 65 8e 22 26 97 03 5c 94 08 e8 e8 58 bc 34 ea d5 41 7b 17 84 18 64 c0 c0 0f 0c 97 55 c1 1b e3 4a 77 08 cd f0 94 02 e7 19 ab a7 38 a9 a4 14 66 d1 35 42 c9 b0 2f 29 2b 1c 46 09 1e 28 96 e3 cc f8 02 26 d1 ea fd 40 4d 7b b2 5b f4 96 ed 59 59 a1 08 cf 3a a4 05 eb 68 b2 eb 82 fb 4a 0a 4d d7 58 44 51 b4 1b 64 df 66 40 71 0d 14 ad 88 e6 17 ae 4c a9 85 87 b3 64 4f 67 f4 8d 1a 17 eb f5 ba 0b 1d 95 40 ef 57 Data Ascii: Yn6P0S4-mSti(Y$9#%R')v :w:Ye&?RaP""X{>bO23UE*Sq@8}c\|K9-*Uzmgu=D}AOYl$YzF@ZH#l/oOS\~Ur$Lx Wj"xbFf5Mo(+$,=hLn2cqd4{8{0N?8JL,2[a,8x"}T!k5Yulq@*h2O%S}mKYn-Z=I"9,U>K$d!`1oH 9 ft ibF.+`2\>~?I.W{=-H)2r{W0rR~<wn=[+(5EPE_d}2?+<{>gw58g%N'Y~FmU@YKhq"4~6e"&\X4A{dUJw8f5B/)+F(&@M{[YY:hJMXDQdf @qLdOg@W
Feb 3, 2021 19:50:19.443145037 CET	2368	OUT	GET /uploads/slider/c4ca4238a0b923820dcc509a6f75849b/slider1-1551387341.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.605907917 CET	2457	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 20:04:04 GMT Accept-Ranges: bytes Content-Length: 494639 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 34 36 35 32 44 39 43 41 33 33 42 33 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 34 36 35 32 44 39 43 39 33 33 42 33 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:4652D9CA33B311E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:4652D9C933B311E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49776	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.160346985 CET	2334	OUT	GET /images/logo.png HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.323482037 CET	2341	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:16 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 02 Dec 2019 19:44:30 GMT Accept-Ranges: bytes Content-Length: 12670 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:16 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=300 Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 0e 00 00 00 8b 08 06 00 00 00 90 bb 77 7a 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 82 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 65 31 64 30 65 32 38 33 2d 65 66 39 36 2d 34 32 35 61 2d 38 33 31 38 2d 38 33 31 35 62 32 62 62 34 34 37 62 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 35 37 44 37 42 46 37 41 30 44 36 30 31 31 45 41 42 41 33 46 38 35 32 30 39 34 38 31 37 37 35 30 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 37 44 37 42 46 37 39 30 44 36 30 31 31 45 41 42 41 33 46 38 35 32 30 39 34 38 31 37 37 35 30 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 42 38 41 31 44 30 33 39 37 41 31 45 22 Data Ascii: PNGIHDRwztEXtSoftwareAdobe ImageReadyqe<iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0 MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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:OriginalDocumentID="xmp.did:e1d0e283-ef96-425a-8318-8315b2bb447b" xmpMM:DocumentID="xmp.did:57D7BF7A0D6011EABA3F852094817750" xmpMM:InstanceID="xmp.iid:57D7BF790D6011EABA3F852094817750" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:018011740720681180 83B8A1D0397A1E"
Feb 3, 2021 19:50:19.444485903 CET	2369	OUT	GET /images/up-arrow.png HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/css/default.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.607503891 CET	2471	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:54:04 GMT Accept-Ranges: bytes Content-Length: 1786 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=299 Connection: Keep-Alive Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 23 00 00 00 35 08 06 00 00 00 cb 56 52 df 00 00 06 c1 49 44 41 54 78 da ed 58 07 4c 54 59 14 9d 30 b0 03 2b 60 81 b5 04 5c 6c 58 92 19 4d 34 ba 0b 64 17 43 54 34 b8 88 32 62 c3 82 88 43 22 82 05 14 0b 23 e0 88 a8 14 6b 62 62 89 b8 88 d8 a2 18 13 5b 10 bb 31 51 08 b1 a1 06 81 11 34 82 a2 14 41 98 81 bb e7 7e e7 cf da 45 ea 26 cb 4d 5e fe 94 f7 df 3b ef de 73 ee 9f 39 12 49 d3 63 a0 99 99 d9 30 5c 2d 24 6d 18 52 80 08 ea d5 ab 57 8e 9b 9b 5b b1 8f 8f 4f 9a 97 97 57 df b6 00 f2 93 4c 26 0b 93 cb e5 35 21 21 21 94 9a 9a 4a 69 69 69 b4 73 e7 4e ad 46 a3 f9 bd 35 81 58 76 e8 d0 61 cb d0 a1 43 6b 57 af 5e 4d 37 6e dc a0 d7 af 5f 53 45 45 05 3d 7c f8 90 92 93 93 4b d5 6a b5 47 6b 00 f9 c5 d2 d2 32 d9 c5 c5 85 d6 af 5f 4f 59 59 59 f4 f6 ed 5b 12 a3 b6 b6 96 0a 0a 0a e8 c8 91 23 55 b1 b1 b1 01 2d 09 c4 d1 c6 c6 26 7d d4 a8 51 b4 75 eb 56 ba 7f ff 3e 55 57 57 53 7d 7d 3d d5 d5 d5 09 83 5f eb f5 7a 7a f6 ec 19 9d 3c 79 52 07 40 51 2d 01 c4 a5 47 8f 1e 99 20 28 ed d9 b3 87 72 73 73 a9 a6 a6 46 d8 b8 b8 b8 98 f2 f3 f3 f5 8f 1e 3d aa 7b f5 ea 95 f0 99 f8 f9 d9 b3 67 eb e2 e3 e3 ff 66 b2 37 8f 64 a4 52 6f 07 07 87 3c 5f 5f 5f 3a 74 e8 10 3d 7d fa 94 74 3a 9d 90 89 17 2f 5e 50 5e 5e 5e 19 46 f8 89 13 27 c2 4e 9f 3e 5d f5 fc f9 73 01 0c 7f cf 5c ba 7c f9 32 6d db b6 ed a2 a7 a7 a7 55 53 70 98 40 ba fe 8e 8e 8e 45 2a 95 8a 4e 9d 3a 25 6c ce 1b 31 37 8a 8a 8a 18 48 f9 93 27 4f 82 c5 1b a0 aa 09 98 f7 86 79 c3 73 b8 6c 95 95 95 74 fb f6 6d da bd 7b 77 b6 bf bf bf 43 63 80 98 23 d4 0a 85 42 bf 64 c9 12 4a 4f 4f 27 2e 01 9f 96 79 c2 d9 01 90 02 00 f9 eb d3 1b 77 ed da 35 ec d8 b1 63 da c7 8f 1f 0b a5 e4 e0 7b ee de bd 4b f8 4e 1b 1a 1a ea f4 23 40 6c a1 98 ed c3 87 0f d7 af 59 b3 86 6e de bc 49 e5 e5 e5 02 10 3e 25 9f 1a 40 ee 00 c8 9f 5f 5b 60 df be 7d 7d 8f 1e 3d 9a 7d ef de 3d 01 08 07 03 63 80 07 0e 1c 28 c3 ba 3e 0d 01 62 df b1 63 c7 54 57 57 57 da b8 71 23 65 67 67 53 55 55 95 b0 58 59 59 99 00 04 20 32 00 66 e0 f7 16 ca c8 c8 e8 84 b2 9d e3 12 f1 21 b8 64 cc 35 ad 56 4b 00 5a 8d f5 43 be 75 bf c2 d6 d6 f6 d2 d8 b1 63 69 c7 8e 1d 94 93 93 43 ef de bd 13 80 94 96 96 b2 62 38 23 29 38 9d 7d 43 53 7c f8 f0 61 69 4a 4a ca de ab 57 af d6 33 99 39 bb cc 39 26 39 b8 a5 03 a0 b8 2f 29 cd 19 d2 7d a0 54 2a 29 29 29 89 4f 2f 10 90 6f 2e 29 29 11 81 24 02 88 75 63 08 88 b2 69 2e 5c b8 a0 e3 b5 44 a5 bd 7c f9 92 ce 9f 3f 5f bf 79 f3 e6 d4 85 0b 17 ca c4 b9 bf 76 ed da f5 da 94 29 53 b8 73 0a 2a e1 74 32 18 3e 01 40 54 00 5c c4 ad 5b b7 7e 6e 8a 34 0f 1e 3c 18 78 e6 cc 99 4a 71 7d 06 c4 a5 bf 7e fd 3a 3f db Data Ascii: PNGIHDR#5VRIDATxXLTY0+`\lXM4dCT42bC"#kbb[1Q4A~E&M^;s9Ic0\-$mRW[OWL&5!!!JiiisNF 5XvaCkW^M7n_SEE=\|KjGk2_OYYY[#U-&}QuV>UWWS}}=_zz<yR@Q-G (rssF={gf7dRo<___:t=}t:/^P^^^F'N>]s \|2mUSp@E*N:%l17H'Oysltm{wCc#BdJOO'.yw5c{KN#@IYnI>%@_[`}}=}=c(>bcTWWWq#eggSUUXYY 2f!d5VKZC uciCb8#)8}CS\|aiJJW399&9/)}T*)))O/o.))$uci.\D|?_yv)Ss*t2>@T\{~n4<xJq}~:?
Feb 3, 2021 19:50:19.693341970 CET	2492	OUT	GET /images/bull.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.856069088 CET	2574	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:21 GMT Accept-Ranges: bytes Content-Length: 18566 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=298 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 38 42 41 30 32 42 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 38 42 41 30 32 41 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:248BA02B33B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:248BA02A33B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:
Feb 3, 2021 19:50:20.133166075 CET	2785	OUT	GET /css/fonts/opensans-regular.woff HTTP/1.1 Host: eriglobal.com Connection: keep-alive Origin: http://eriglobal.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://eriglobal.com/css/default.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:20.295638084 CET	2968	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:17 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:54:39 GMT Accept-Ranges: bytes Content-Length: 24784 Cache-Control: max-age=604800 Expires: Wed, 10 Feb 2021 18:50:17 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Keep-Alive: timeout=20, max=297 Connection: Keep-Alive Content-Type: application/x-font-woff Data Raw: 77 4f 46 46 00 01 00 00 00 00 60 d0 00 13 00 00 00 00 b0 90 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 68 49 7a ca 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 17 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a2 00 00 09 98 2c 1a 16 58 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 5e 88 92 4f 53 2f 32 00 00 07 0c 00 00 00 60 00 00 00 60 a0 e5 99 86 63 6d 61 70 00 00 07 6c 00 00 01 86 00 00 01 da cf 40 58 a0 63 76 74 20 00 00 08 f4 00 00 00 46 00 00 00 46 13 89 0d 09 66 70 67 6d 00 00 09 3c 00 00 01 b1 00 00 02 65 53 b4 2f a7 67 61 73 70 00 00 0a f0 00 00 00 10 00 00 00 10 00 15 00 23 67 6c 79 66 00 00 0b 00 00 00 4c 90 00 00 90 f8 39 96 b1 5c 68 65 61 64 00 00 57 90 00 00 00 33 00 00 00 36 0b ee b0 f8 68 68 65 61 00 00 57 c4 00 00 00 1f 00 00 00 24 0f 73 06 3f 68 6d 74 78 00 00 57 e4 00 00 02 37 00 00 03 a6 da 43 58 aa 6c 6f 63 61 00 00 5a 1c 00 00 01 cc 00 00 01 d6 6d 5c 4a e0 6d 61 78 70 00 00 5b e8 00 00 00 20 00 00 00 20 02 07 01 97 6e 61 6d 65 00 00 5c 08 00 00 02 06 00 00 04 7e 51 48 9d 8b 70 6f 73 74 00 00 5e 10 00 00 01 ed 00 00 02 e5 1a 78 32 a8 70 72 65 70 00 00 60 00 00 00 00 c8 00 00 01 76 40 c8 ad ce 77 65 62 66 00 00 60 c8 00 00 00 06 00 00 00 06 f5 f0 56 b0 00 00 00 01 00 00 00 00 cc 3d a2 cf 00 00 00 00 c9 35 31 8b 00 00 00 00 d2 d6 a6 6f 78 da 63 60 64 60 60 e0 03 62 09 06 10 60 62 60 04 c2 97 40 cc 02 e6 31 00 00 0e 4d 01 1c 00 00 78 da ad 96 4b 6c 54 55 18 c7 ff 33 9d 61 c6 82 96 aa d1 f8 08 1a 32 36 b5 06 8d 0d 49 db b1 b0 6a da 5a 0d 96 69 8b 83 0e 8a 0f e2 02 42 42 63 48 4c 13 16 85 81 b8 30 21 06 2b 39 3c 6a 0a 4c a1 d0 59 90 52 9a f2 32 4c 57 2c dc e1 69 6d e3 ca e5 49 57 c4 05 21 8e bf 73 db 29 e0 48 d5 c4 7c f9 e5 dc 39 f7 bb df e3 7f ce 3d 73 15 92 54 a9 6e 7d aa 48 4b eb bb dd 7a fe b3 af 7a 77 a9 e6 8b de 1d 3b 55 bf eb 93 2f 77 6b a3 22 f8 a8 58 94 f7 fd 37 d7 a1 9d 3b 7a 77 2b ee af 02 22 0a 07 63 5c a1 78 6f e0 b9 5d b7 74 2b 74 38 34 10 ba 03 77 c3 e9 70 0e a6 c3 bf 86 73 15 ab c3 e9 8a 7d 30 16 f9 29 72 2f 72 2f 9c 8b ce af f8 2d 74 38 f6 4c ac 36 96 82 cf b9 da 0b fe 77 6d ec c7 58 2a 9e 8c 27 63 7b e3 49 e2 dd bd 6f 44 cb c1 82 a5 1f 34 e2 06 16 9d af d8 17 c4 29 59 ed c3 16 df 0e 49 4f 78 3a 3a 4f a5 77 82 aa 07 02 de 54 a2 b8 47 0d 7a 55 4d 90 84 66 3d ad 96 62 5e ad c5 ac da a0 1d 3a 8a 05 75 c2 66 48 f1 bb 8b b1 9b b1 87 71 0b a4 a1 9f 38 fb e1 00 64 e1 20 1c 82 41 e2 0d e1 7b 8a 98 a7 e1 0c e4 60 18 ce c2 39 ee 8d c0 79 b8 00 a3 30 06 97 60 1c 2e c3 04 4c c2 15 f2 5c 85 6b Data Ascii: wOFF`FFTMhIzGDEF GPOS,XGSUB^OS/2``cmapl@Xcvt FFfpgm<eS/gasp#glyfL9\headW36hheaW$s? hmtxW7CXlocaZm\Jmaxp[ name\~QHpost^x2prep`v@webf`V=51oxc`d``b`b`@1MxKITU3a26IjZiBBcHL0!+9<jLYR2 LW,imIW!s)H|9=sTn}HKzzw;U/wk"X7;zw+"c\xo]t+t84wps}0)r/r/-t8L6wmX*'c{IoD4)YIOx::OwTGzUMf=b^:ufHq8d A{`9y0`.L\k

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49778	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:19.349519014 CET	2354	OUT	GET /uploads/maxresdefault.jpg HTTP/1.1 Host: eriglobal.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Referer: http://eriglobal.com/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: WDESS=dceff53b471f6d34d7c866315f5aa2b5; session=8b6bfc69995572d35be50026df1c0741; lang=english

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Feb 3, 2021
19:50:19.514218092 CET</td><td>2401</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 03 Feb 2021 18:50:16 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Mon, 01 Jul 2019 18:11:13 GMT
Accept-Ranges: bytes
Content-Length: 452028
Cache-Control: max-age=2419200
Expires: Wed, 03 Mar 2021 18:50:16 GMT
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge,chrome=1
Keep-Alive: timeout=20, max=300
Content-Type: image/jpeg
Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 64 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 02 02 02 02 02 02 02 02 02 02 02 03 03 03 03 03 03 03 03 03 01 01 01 01 01 01 01 02 01 01 02 02 02 01 02 02 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 ff c0 00 11 08 02 ce 04 fc 03 01 11 00 02 11 01 03 11 01 ff c4 00 ce 00 00 00 06 03 01 01 01 00 00 00 00 00 00 00 00 00 00 01 02 03 06 07 04 05 08 09 0a 0b 01 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 03 01 02 04 05 06 07 08 10 00 01 03 03 02 04 03 05 06 04 04 04 04 02 01 15 01 02 03 04 11 05 06 00 12 21 31 13 07 41 51 14 61 91 22 15 08 71 81 a1 d1 32 52 f0 b1 23 16 e1 42 17 09 62 72 33 24 c1 92 a2 25 f1 82 43 34 d2 53 26 18 e2 63 35 36 b2 c2 f2 73 54 27 83 44 45 95 d6 28 11 00 02 02 01 03 03 03 02 03 06 05 03 03 03 02 07 00 01 11 02 03 21 31 12 41 51 04 61 13 05 71 22 f0 81 32 91 a1 b1 c1 14 06 d1 42 23 33 15 e1 f1 52 62 72 24 82 53 34 16 43 c2 73 25 35 07 d2 63 ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 b6 91 c4 7d ff 00 f8 0d 7e cb bd d3 47 e3 f1 0e fe a1 ff 00 28 fe 67 59 5e ef ea 09 a5 bb 12 12 7c 8f b8 e9 94 69 2d 42 50 74 34 e4 7d da 75 6c b8 b4 1b 8b 47 2f bf ff 00 01 aa 4a 5b 80 4b fd 40 1f 21 fc ce ab cd 4c 15 e6 a6 01 b5 1f bb f1 1a b4 c6 e5 c3 a2 47 10 a1 51 c4 0a 8e 63 8e a8 ee b5 5a 90 27 aa af 24 fb 8f e7 a5 40 34 96 e0 2e 13 ce 9 e 5e 3f 9e 9b 48 4b f3 17 6b d6 1a 52 23 c6 ba 6f 25 c2 3d 45 24 da d1 30 81 a1 af 91 ae b3 3d d8 da 52 54 b9 91 ce aa b c 93 ee 3f 9e a2 06 34 96 e1 87 09 22 b4 e6 07 8f 9f db a6 d2 15 45 bb d7 65 23 fa bf 25 c6 3d 4a 08 3c 8d 39 f1 a6 b3 bd c9 e8 37 bd 7f b7 f0 3f 9e 82 25 80 29 64 81 b7 99 03 91 d0 12 c7 b6 ab f6 ab dc 75 04 ca 09 49 56 d5 7c 2a e4 7c 0f 96 80 7b 18 db 55 fb 4f b8 ea c5 f1 b4 ab af 71 68 a8 22 a0 f3 1c 69 c0 7d a7 55 63 95 97 16 87 8a 93 fb 87 bc 68 14 d3 81 25 42 86 84 56 87 c4 6a 44 3a 55 39 ea 25 2e 1a 8e 5c c7 9f 9f db a6 d2 12 d4 99 72 64 15 92 0f 2f e3 ef d5 a5 44 92 37 a4 d9 cb 94 48 4a e4 7e c3 fc b5 00 f6 09 a4 ab 69 f8 4f ea 3e 07 c8 69 95 69 2d 59 54 12 d2 ae a2 4d 0f f9 7c 0f ee 3a 75 72 55 51 a9 d4 3a 8e 69 72 bb 92 02 78 1a 73 a1 d1 2b b8 0d 15 af f6 fe 07 f3 d5 6e d3 5a 32 25 80 a9 64 6d
Data Ascii: ExifII*DuckydAdobed!1AQa"q2R#Bbr3$%C4S&c56sT'DE(!1AQaq"2B#3Rbr$S4Cs%5c?}~G(gY^|i-BPt4}ul G/J[K@!LGQcZ'$@4.^?HKkR#o%=E$0=RT?4"Ee#%=J<97?%)duIV|*|{UOqh"i}Uch%BVjD:U9%.\rd/D7HJ~iO>ii-YTM|:urUQ :irxs+nZ2%dm</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49789	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:22.463912964 CET	4510	OUT	GET /images/ico/favicon.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: eriglobal.com

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:22.630165100 CET	4512	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Mon, 04 Mar 2019 19:52:51 GMT Accept-Ranges: bytes Content-Length: 1823 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:20 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f f3 ff 61 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 24 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 53 36 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 41 34 38 45 41 46 43 39 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 41 34 38 45 41 46 43 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 38 36 33 43 36 35 39 32 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 41 34 38 45 41 46 43 38 36 30 44 37 31 31 45 33 38 36 33 35 41 45 39 34 43 44 31 34 38 39 31 31 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d 70 6d 65 74 61 3e 20 3c 3f 78 70 61 63 6b 65 74 20 65 6e 64 3d 22 72 Data Ascii: PNGIHDRatEXtSoftwareAdobe ImageReadyqe<$iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0 MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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 CS6 (Macintosh)" xmpMM:Instan ceID="xmp.iid:A48EAFC960D711E38635AE94CD148911" xmpMM:DocumentID="xmp.did:A48EAFCA60D711E3 8635AE94CD148911"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:863C659260D711E38635AE94CD148911" st Ref:documentID="xmp.did:A48EAFC860D711E38635AE94CD148911"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <? xpacket end="r
Feb 3, 2021 19:50:22.639178991 CET	4513	OUT	GET /images/bull.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: eriglobal.com

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:22.805589914 CET	4529	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:20 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:21 GMT Accept-Ranges: bytes Content-Length: 18566 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:20 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 38 42 41 30 32 42 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 38 42 41 30 32 41 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 64 62 39 39 38 31 39 2d 37 35 64 31 2d 31 31 37 63 2d 62 33 63 64 2d 64 34 65 35 64 62 39 30 63 38 33 66 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:248BA02B33B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:248BA02A33B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:8db99819-75d1-117c-b3cd-d4e5db90c83f"/></rdf:Description
Feb 3, 2021 19:50:22.983989000 CET	4574	OUT	GET /images/cuild2.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: eriglobal.com

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:23.150298119 CET	4593	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:20 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:29 GMT Accept-Ranges: bytes Content-Length: 25396 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:20 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 39 45 38 32 37 45 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 38 42 41 30 33 32 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 64 62 39 39 38 31 39 2d 37 35 64 31 2d 31 31 37 63 2d 62 33 63 64 2d 64 34 65 35 64 62 39 30 63 38 33 66 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:249E827E33B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:248BA03233B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:8db99819-75d1-117c-b3cd-d4e5db90c83f"/> </rdf:Description

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49790	68.233.236.236	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:22.494864941 CET	4510	OUT	GET /images/logo.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: eriglobal.com

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:22.658075094 CET	4515	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Mon, 02 Dec 2019 19:44:30 GMT Accept-Ranges: bytes Content-Length: 12670 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:20 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 0e 00 00 00 8b 08 06 00 00 00 90 bb 77 7a 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 82 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 65 31 64 30 65 32 38 33 2d 65 66 39 36 2d 34 32 35 61 2d 38 33 31 38 2d 38 33 31 35 62 32 62 62 34 34 37 62 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 35 37 44 37 42 46 37 41 30 44 36 30 31 31 45 41 42 41 33 46 38 35 32 30 39 34 38 31 37 37 35 30 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 37 44 37 42 46 37 39 30 44 36 30 31 31 45 41 42 41 33 46 38 35 32 30 39 34 38 31 37 37 35 30 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 42 38 41 31 44 30 33 39 37 41 31 45 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 61 30 37 Data Ascii: PNGIHDRwztEXtSoftwareAdobe ImageReadyqe<iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0 MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <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:OriginalDocumentID="xmp.did:e1d0e283-ef96-425a-8318-8315b2bb447b" xmpMM:DocumentID="xmp.did:57D7BF7A0D6011EABA3F852094817750" xmpMM:InstanceID="xmp.iid:57D7BF790D6011EABA3F852094817750" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:01801174072068118083B8A1D0397A1E" stRef:documentID="adobe:docid:photoshop:1a07
Feb 3, 2021 19:50:22.667021990 CET	4527	OUT	GET /images/building.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: eriglobal.com

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:22.832017899 CET	4544	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:20 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:20 GMT Accept-Ranges: bytes Content-Length: 29099 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:20 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 38 42 41 30 32 46 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 38 42 41 30 32 45 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 64 62 39 39 38 31 39 2d 37 35 64 31 2d 31 31 37 63 2d 62 33 63 64 2d 64 34 65 35 64 62 39 30 63 38 33 66 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e Data Ascii: ExifII*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:248BA02F33B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:248BA02E33B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:8db99819-75d1-117c-b3cd-d4e5db90c83f"/></rdf:Description
Feb 3, 2021 19:50:23.011388063 CET	4588	OUT	GET /images/build3.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: eriglobal.com

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:23.174849987 CET	4610	IN	HTTP/1.1 200 OK Date: Wed, 03 Feb 2021 18:50:20 GMT Server: Apache Last-Modified: Mon, 04 Mar 2019 19:52:17 GMT Accept-Ranges: bytes Content-Length: 15822 Cache-Control: max-age=2419200 Expires: Wed, 03 Mar 2021 18:50:20 GMT Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-UA-Compatible: IE=edge,chrome=1 Content-Type: image/jpeg Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 8f 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 62 61 34 66 36 34 31 36 2d 31 34 38 38 2d 34 32 64 31 2d 62 61 61 66 2d 37 36 62 34 65 34 35 62 65 35 64 63 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 34 39 45 38 32 38 32 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 34 39 45 38 32 38 31 33 33 42 39 31 31 45 39 39 38 30 32 42 41 39 37 30 33 30 32 31 37 42 38 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 35 66 35 37 64 34 64 64 2d 65 30 31 62 2d 34 33 32 33 2d 39 39 36 38 2d 61 33 34 64 30 32 39 38 61 30 34 30 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 64 62 39 39 38 31 39 2d 37 35 64 31 2d 31 31 37 63 2d 62 33 63 64 2d 64 34 65 35 64 62 39 30 63 38 33 66 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e Data Ascii: Exif|*Ducky<http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <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:OriginalDocumentID="xmp.did:ba4f6416-1488-42d1-baaf-76b4e45be5dc" xmpMM:DocumentID="xmp.did:249E828233B911E99802BA97030217B8" xmpMM:InstanceID="xmp.iid:249E828133B911E99802BA97030217B8" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:5f57d4dd-e01b-4323-9968-a34d0298a040" stRef:documentID="adobe:docid:photoshop:8db99819-75d1-117c-b3cd-d4e5db90c83f"/> </rdf:Description

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49864	199.30.234.249	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Feb 3, 2021 19:50:42.109424114 CET	6262	OUT	GET / HTTP/1.1 Host: www.zixcorp.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Feb 3, 2021 19:50:42.276321888 CET	6263	IN	HTTP/1.0 302 Found Location: https://www.zixcorp.com/ Server: BigIP Connection: Keep-Alive Content-Length: 0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:02.441752911 CET	63.71.15.50	443	192.168.2.6	49726	CN=web1.zixmail.net, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Jun 25 22:58:10 CEST 2019 Tue Nov 29 17:42:17 CET 2016	Fri Jun 25 23:28:08 CEST 2021 Mon Dec 02 05:00:00 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		
Feb 3, 2021 19:50:02.441854000 CET	63.71.15.50	443	192.168.2.6	49727	CN=web1.zixmail.net, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Jun 25 22:58:10 CEST 2019 Tue Nov 29 17:42:17 CET 2016	Fri Jun 25 23:28:08 CEST 2021 Mon Dec 02 05:00:00 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		
Feb 3, 2021 19:50:02.519972086 CET	63.71.15.50	443	192.168.2.6	49728	CN=web1.zixmail.net, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Jun 25 22:58:10 CEST 2019 Tue Nov 29 17:42:17 CET 2016	Fri Jun 25 23:28:08 CEST 2021 Mon Dec 02 05:00:00 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		
Feb 3, 2021 19:50:07.439496040 CET	63.71.15.50	443	192.168.2.6	49753	CN=web1.zixmail.net, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Jun 25 22:58:10 CEST 2019 Tue Nov 29 17:42:17 CET 2016	Fri Jun 25 23:28:08 CEST 2021 Mon Dec 02 05:00:00 CET 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:07.440071106 CET	63.71.15.50	443	192.168.2.6	49754	CN=web1.zixmail.net, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Jun 25 22:58:10 CEST 2019 Tue Nov 29 17:42:17 CET 2016	Fri Jun 25 23:28:08 CEST 2021 Mon Dec 02 05:00:00 CET 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		
Feb 3, 2021 19:50:22.982892990 CET	199.30.234.249	443	192.168.2.6	49793	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020 Mon Dec 15 16:25:03 CET 2014	Wed Nov 10 18:25:08 CET 2021 Tue Oct 15 17:55:03 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:22.982966900 CET	199.30.234.249	443	192.168.2.6	49792	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020 Mon Dec 15 16:25:03 CET 2014	Wed Nov 10 18:25:08 CET 2021 Tue Oct 15 17:55:03 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:23.052988052 CET	199.30.234.249	443	192.168.2.6	49794	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020 Mon Dec 15 16:25:03 CET 2014	Wed Nov 10 18:25:08 CET 2021 Tue Oct 15 17:55:03 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:26.230935097 CET	3.213.190.117	443	192.168.2.6	49803	CN=www.bugherd.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 16 04:25:21 CET 2021	Fri Apr 16 05:25:21 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
							Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 3, 2021 19:50:34.776097059 CET	185.63.144.5	443	192.168.2.6	49823	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 06 01:00:00 CET 2021	Tue Jul 06 01:59:59 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
							Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Feb 3, 2021 19:50:35.685774088 CET	3.229.202.186	443	192.168.2.6	49826	CN=driftqa.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Jun 18 02:00:00 CEST 2020	Sun Jul 18 14:00:00 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:35.803360939 CET	54.72.203.0	443	192.168.2.6	49827	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Mar 26 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Apr 26 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 3, 2021 19:50:39.956163883 CET	199.30.234.249	443	192.168.2.6	49837	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020 Mon Dec 15 16:25:03 CET 2014	Wed Nov 10 18:25:08 CET 2021 Tue Oct 15 17:55:03 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:40.124736071 CET	199.30.234.249	443	192.168.2.6	49838	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020 Mon Dec 15 16:25:03 CET 2014	Wed Nov 10 18:25:08 CET 2021 Tue Oct 15 17:55:03 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:40.128249884 CET	54.147.21.139	443	192.168.2.6	49841	CN=drift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 23 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 3, 2021 19:50:40.320301056 CET	34.120.207.148	443	192.168.2.6	49846	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Apr 14 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sat Apr 24 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Feb 3, 2021 19:50:40.356658936 CET	52.215.8.160	443	192.168.2.6	49845	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Mar 26 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Apr 26 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 3, 2021 19:50:40.761130095 CET	99.86.167.41	443	192.168.2.6	49851	CN=*.company-target.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jun 19 18:48:33 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Wed Aug 18 20:47:01 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Feb 3, 2021 19:50:40.960043907 CET	18.215.11.20	443	192.168.2.6	49852	CN=drift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 23 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 3, 2021 19:50:41.559750080 CET	100.24.186.63	443	192.168.2.6	49855	CN=drift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 23 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 3, 2021 19:50:41.588965893 CET	54.198.218.148	443	192.168.2.6	49856	CN=wschat.api.drift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 13 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	74ad8ec6876e2e3366bfd566581ca7e8
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:41.623903036 CET	54.85.240.191	443	192.168.2.6	49857	CN=drift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 23 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	74ad8ec6876e2e3366bfd566581ca7e8
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 3, 2021 19:50:41.639713049 CET	18.205.49.143	443	192.168.2.6	49858	CN=drift.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 23 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:42.885646105 CET	199.30.234.249	443	192.168.2.6	49867	CN=www.zixcorp.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Wed Nov 13 21:24:10 CET 2019	Sat Dec 11 21:54:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		
Feb 3, 2021 19:50:43.048178911 CET	199.30.234.249	443	192.168.2.6	49869	CN=www.zixcorp.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Wed Nov 13 21:24:10 CET 2019	Sat Dec 11 21:54:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=AffirmTrust Extended Validation CA - EV1, OU=See www.affirmtrust.com/repository, O=AffirmTrust, C=CA	CN=AffirmTrust Commercial, O=AffirmTrust, C=US	Tue Nov 29 17:42:17 CET 2016	Mon Dec 02 05:00:00 CET 2030		
Feb 3, 2021 19:50:44.534210920 CET	199.30.234.249	443	192.168.2.6	49874	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:46.446790934 CET	3.213.190.117	443	192.168.2.6	49889	CN=www.bugherd.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 16 04:25:21 CET 2021	Fri Apr 16 05:25:21 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:46.487003088 CET	199.30.234.249	443	192.168.2.6	49884	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:46.487711906 CET	199.30.234.249	443	192.168.2.6	49885	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:46.497158051 CET	199.30.234.249	443	192.168.2.6	49887	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:46.497206926 CET	199.30.234.249	443	192.168.2.6	49886	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:46.499102116 CET	199.30.234.249	443	192.168.2.6	49888	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		
Feb 3, 2021 19:50:56.859980106 CET	199.30.234.249	443	192.168.2.6	49907	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020	Wed Nov 10 18:25:08 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 3, 2021 19:50:56.871733904 CET	199.30.234.249	443	192.168.2.6	49908	CN=zix.com, SERIALNUMBER=3052178, OID.2.5.4.15=Private Organization, O="ZixCorp Systems, Inc.", OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, L=Dallas, ST=Texas, C=US CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 10 18:25:09 CET 2020 Mon Dec 15 16:25:03 CET 2014	Wed Nov 10 18:25:08 CET 2021 Tue Oct 15 17:55:03 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Entrust Certification Authority - L1M, OU="(c) 2014 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Dec 15 16:25:03 CET 2014	Tue Oct 15 17:55:03 CEST 2030		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6956 Parent PID: 1420

General

Start time:	19:49:57
Start date:	03/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://web1.zixmail.net/s/e?b=4eri&m=ABCQiFe9wlqI9X9vKBvYvvDp&c=ABBhRV19Ad0FHPsNXID7AQI6&em=new%2eclaimsnotices%40jamesriverins%2ecom'
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 7128 Parent PID: 6956

General

Start time:	19:49:58
Start date:	03/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,991956672690595382,7383702837834195658,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: chrome.exe PID: 6460 Parent PID: 6956

General

Start time:	19:50:35
Start date:	03/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1552,991956672690595382,7383702837834195658,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=2192 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly