Passive (Aggressive) DNS

APRIL LORENZEN
M3AAWG SR TECHNICAL ADVISOR

M3AAWG is a Trusted Environment

What happens in M3AAWG stays in M3AAWG

- What occurs here cannot be shared outside the membership without the written permission of the Executive Director, unless we state the specific session is open to the press and social media.
- See the M3AAWG Meeting Policy at www.m3aawg.org/MeetingPolicy

Treat Everyone with Respect

- Treat all attendees respectfully in and out of sessions. No less will be tolerated.
- See the M3AAWG Conduct Policy at https://www.m3aawg.org/conduct-policy

You agreed to these policies when you registered for the meeting.

For questions, please contact Amy Cadagin at amy@m3aawg.org

Contribute to a Productive Meeting

- Please silence all electronic devices; be courteous to those listening to the presentations
- DO NOT LEAVE YOUR BELONGINGS UNATTENDED. Be aware and cautious at all times

Reminders for Our Worldwide Friends

All meeting content is confidential: No photos, no video, no recording.
Reach out to room monitor staff with questions.

L’ensemble du contenu de la réunion est confidentiel : les photos, vidéos et enregistrements sont interdits. Pour toute question, demandez conseil au personnel.

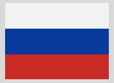
Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.

Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.

会議の内容はすべて機密扱いです。写真やビデオの撮影、録音は禁止されています。質問がある方は、スタッフまでご連絡ください。

所有会议内容均为保密信息：禁止拍照、录像、录音。如有疑问，请咨询职员。

회의에서 다루는 모든 내용은 기밀입니다. 사진 및 동영상 촬영과 녹음은 금지됩니다. 질문이 있으시면 직원에게 문의해 주십시오.



Все содержимое собрания является конфиденциальным: нет фотографий, нет видео, нет записи. Смотрите сотрудников с вопросами.

Code of Conduct

M³AAWG is dedicated to making our meetings and business open to all members and guests and to making it a safe place for all. We do not tolerate harassment of any kind.

We insist that all participants, attendees and meeting staff adhere to a civil demeanor at all times. This includes refraining from inappropriate language, comments and behavior, in person or by electronic communications and/or public or semi-public social media. In accordance with applicable law, M³AAWG prohibits sexual harassment and harassment because of race, color, gender, age, religion, disability, sexual orientation or any other basis protected by federal, state or local law.

Participants, attendees and meeting staff who are being harassed, intimidated, or are dealing with otherwise improper behavior are encouraged to report it immediately to the Executive Director or a Board member without fear of repercussion.

Alternate methods of reporting issues include: contacts listed on the back of your badge, email to the Executive Director, amy@m3aawg.org, or if needed, calling the local police department.

Anyone who is found to be in violation of this policy may be handled in any one or more of these methods, depending on the offense: Warning, Expulsion, Contacting of employer, or Contacting the police or other legal authorities. Actions stronger than a warning will be taken at the discretion of the M³AAWG Board of Directors.

M³AAWG reserves the right to remove any participant or attendee at any time for any reason.

The policy also extends outside of the meeting rooms to include all areas of the meeting hotel and social gatherings sponsored by M³AAWG or M³AAWG member organizations.

Note: You can download this file at https://www.m3aawg.org/conduct-policy

Conduct Violations - Reporting

If You Feel Unsafe: Touching or physical contact of any kind that is unwanted or Physical or verbal threats of any kind

1. Contact **Local Law Enforcement:** In **Brooklyn** call **911**
2. Once you are safe, contact M3AAWG Executive Director or designated Board Officer
3. During the night out, go to the designated Staff table for immediate assistance
4. From the **Upcoming Meetings** page you can find **Safety Information** page: https://www.m3aawg.org/safety-security with further information
5. **Safety Card** available at Registration Desk

If you are <u>not in danger</u> then call or text Executive Director or designated Board Officer (24/7)

Amy Cadagin (+1-618-741-3071) ; Email (amy@m3aawg.org)

Janet Jones (+1-206-498-0495)

Severin Walker (+1-856-496-9862)

Any violations should be reported as soon as possible!

When there is any doubt about the action that should be taken call or text someone on the back of the badge.

Health and Wellness

General Reminders for attendees:

- Face mask to be wore at ALL times
- Wash hands frequently with soap and water for at least 20 seconds.
- If soap and water are not readily available, use an alcohol-based hand sanitizer with at least 60% alcohol. M3AAWG is providing hand sanitizer near the door of each meeting room.
- Avoid touching eyes, nose, and mouth with unwashed hands.
- Avoid close contact with people who are sick.
- Stay home when sick.
- Cover a cough or sneeze with a tissue, then throw the tissue in the trash.
- Clean and disinfect frequently touched objects and surfaces using a regular household cleaning spray or wipe
- We encourage everyone to follow the guidance of the **Centers for Disease Control and Prevention (CDC)** for everyday preventative actions to help prevent the spread of respiratory viruses.

Housekeeping

- **Airmeet –** Access to the most up-to-date agenda and networking.
- **SCHED –** Airmeet link, most up-to-date agenda, technical support and staff contact info.
- **Virtual Help Desk –** Please send a direct message to a M3AAWG Staff
- **In Person Help Desk** - Please see Registration Desk at Salon DE Foyer
- **Virtual Q&A –** Submit your questions to the Speaker in the Airmeet Q&A box.
- **In Person Q&A –** Submit your questions in the Airmeet Q&A box or ask live (please use the microphone in the main aisle so everyone can hear your question)
- **Chat –** Please keep the chat productive, check there for links and reminders.
- **Available for Viewing –** Presentation decks are available (if approved)

Social Media Plans & Policy

- **M³AAWG comms team will provide live posts** across the org social channels during the meeting
- **Members and their PR/comms teams and colleagues are welcome and encouraged to re-post our content**
- Tag @M3AAWG, link to https://m3aawg.org
- General org hashtags: **#m3aawg56 #messaging #malware #cybersecurity #onlineabuse #mobile**
- Due to our confidentiality policies and range of permissions from members/session presenters, members **should not create their own content or originate posts/info from sessions** this week, nor post any info or names/orgs/titles/work product from members and attendees
- If you or your marketing/PR/comms teams want to promote, please have them contact Anne Price, anne@m3aawg.org

OVERVIEW

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- PARTICIPATION - safe for introverts too:

  menti.com and enter 67 29 15 3

- M3AAWG Leadership on Passive DNS
- Why “Passive DNS”?

- Things you can do with Passive DNS
- Cautionary Tales

- Tips - Tricks - Resources

Go to www.menti.com and use the code 67 29 15 3

WHEN DID YOU START USING PASSIVE DNS?

Mentimeter

PIONEER: FLORIAN WEIMER

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Passive DNS Replication

Florian Weimer <fw@deneb.enyo.de>

April 2005

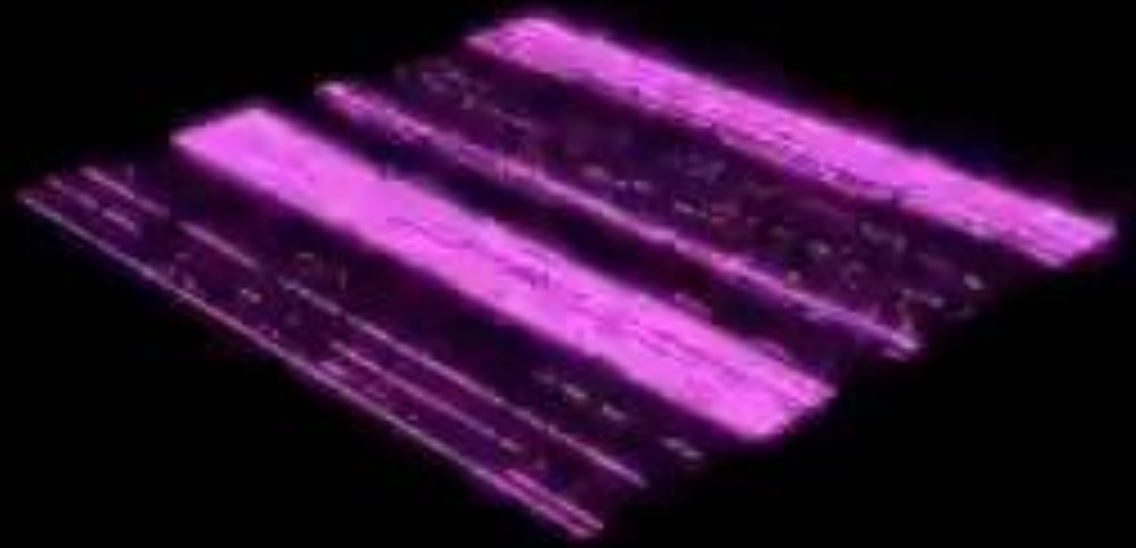
Overview

The domain name system (abbreviated 'DNS') provides a distributed database that maps domain names to record sets (for example, IP addresses). DNS is one of the core protocol suites

APRIL LORENZEN

2006: First presentation on FastFlux in DNS
(invited to SF MAAWG by Joe St Sauver)

2007: Credited as Inventor of NS Reputation
(by MAAWG Sr Technical Advisor David Dagon)




Florian Weimer & April Lorenzen
Introduced Passive DNS to MAAWG Members
MAAWG 2008 Heidelberg, Germany

WORLD-WIDE ADOPTION COMMENCED

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Paul Vixie (BIND, CRON, RPZ)
- Tireless evangelizing by April & Paul

- **Today:**
  - Florian works at RedHat, BFK carries torch
  - Joe St Sauver works at Passive DNS vendor
  - David Dagon (so many Passive DNS projects)
  - David Ulevitch (OpenDNS)
  - Spamhaus / Deteque (M3AAWG Pioneers)
  - NetLab360, many more

Everybody's doin' it …. but why?

Go to www.menti.com and use the code 67 29 15 3

Mentimeter

WHICH PASSIVE DNS SYSTEMS DO YOU USE?

PASSIVE DNS ENABLES:

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Tracking of botnets over time
- Clustering of malicious domain registrations
- History of IPs this domain has used
- History of domains hosted on this IP
- Statistical models for reputation

USE CASES

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Fun (search: sunnyjuly.gq)
  Collaborative Hunting
- Network Protection
- Forensic Investigations
- Footprint
  - Self - reputation and pen testing
  - Vetting of customers and vendors

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Passive (Aggressive) DNS

USE CASE:
MALICIOUS DOMAIN STUDIES

bit.ly/2022zc

Urgent - Please view your recent activity and we'll help you take corrective action #359872

AMEX Online Services .750512

Yesterday at 4:14 PM

Urgent - Please view your recent activity and we'll help you take corrective action #359872

To: undisclosed-recipients:;

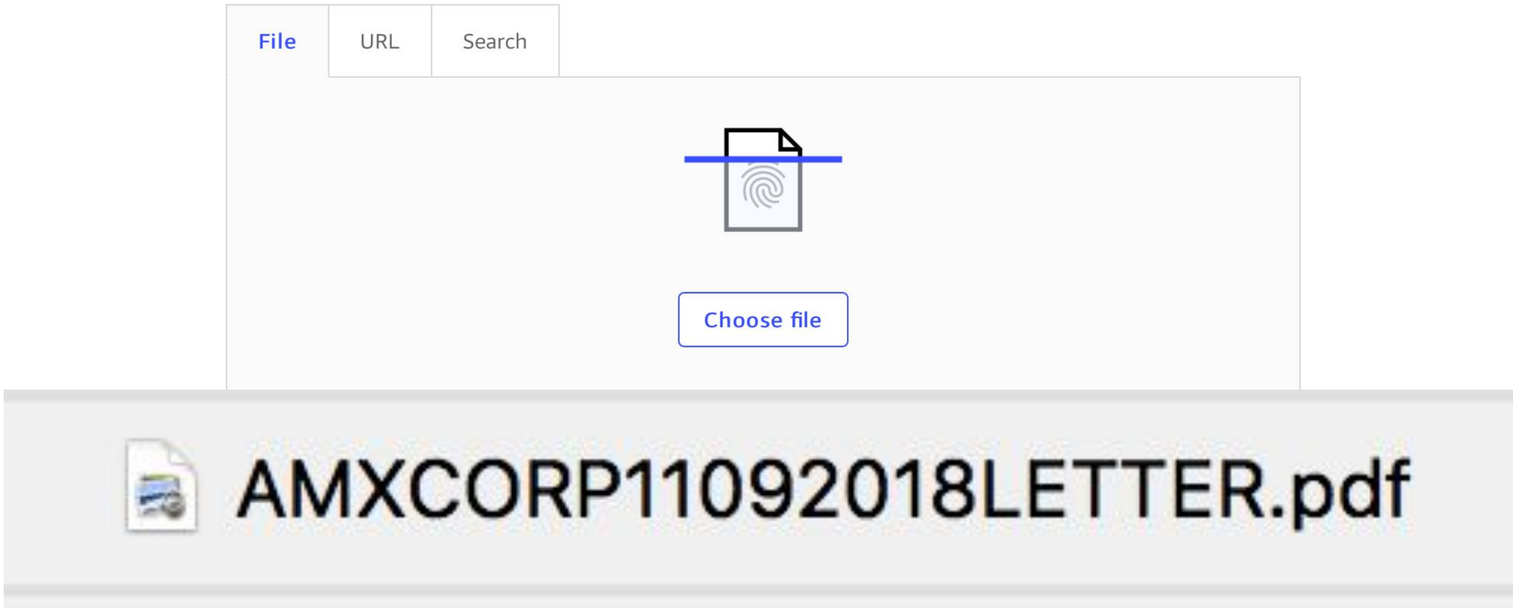
We noticed an Appple Pay™ transaction from an unauthorized unknown device or location on September 11, 2018
We have included the detailed information in attached document in this email message

Sincerely,
American Express.

AMXCORP11092018LETTER.pdf

VirusTotal

Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community.



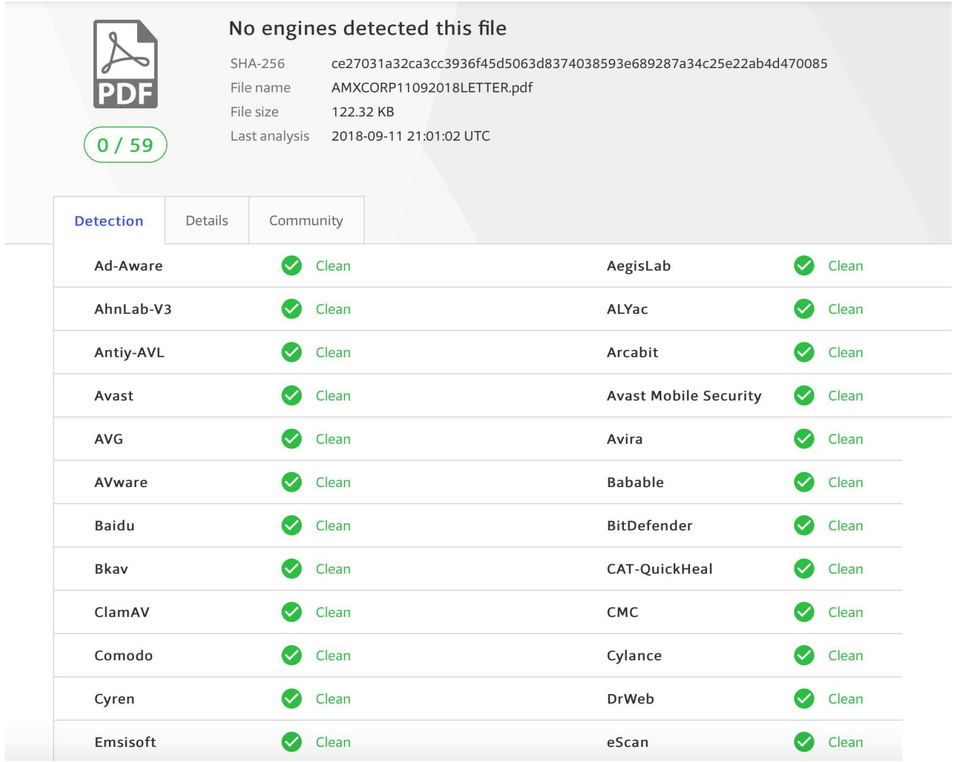
0 / 59

No engines detected this file

SHA-256	ce27031a32ca3cc3936f45d5063d8374038593e689287a34c25e22ab4d470085
File name	AMXCORP11092018LETTER.pdf
File size	122.32 KB
Last analysis	2018-09-11 21:01:02 UTC

Detection | Details | Community

Ad-Aware	Clean	AegisLab	Clean
AhnLab-V3	Clean	ALYac	Clean
Antiy-AVL	Clean	Arcabit	Clean
Avast	Clean	Avast Mobile Security	Clean
AVG	Clean	Avira	Clean
AVware	Clean	Babable	Clean
Baidu	Clean	BitDefender	Clean
Bkav	Clean	CAT-QuickHeal	Clean
ClamAV	Clean	CMC	Clean
Comodo	Clean	Cylance	Clean



No engines detected this file

SHA-256	ce27031a32ca3cc3936f45d5063d8374038593e689287a34c25e22ab4d470085
File name	AMXCORP11092018LETTER.pdf
File size	122.32 KB
Last analysis	2018-09-11 21:01:02 UTC

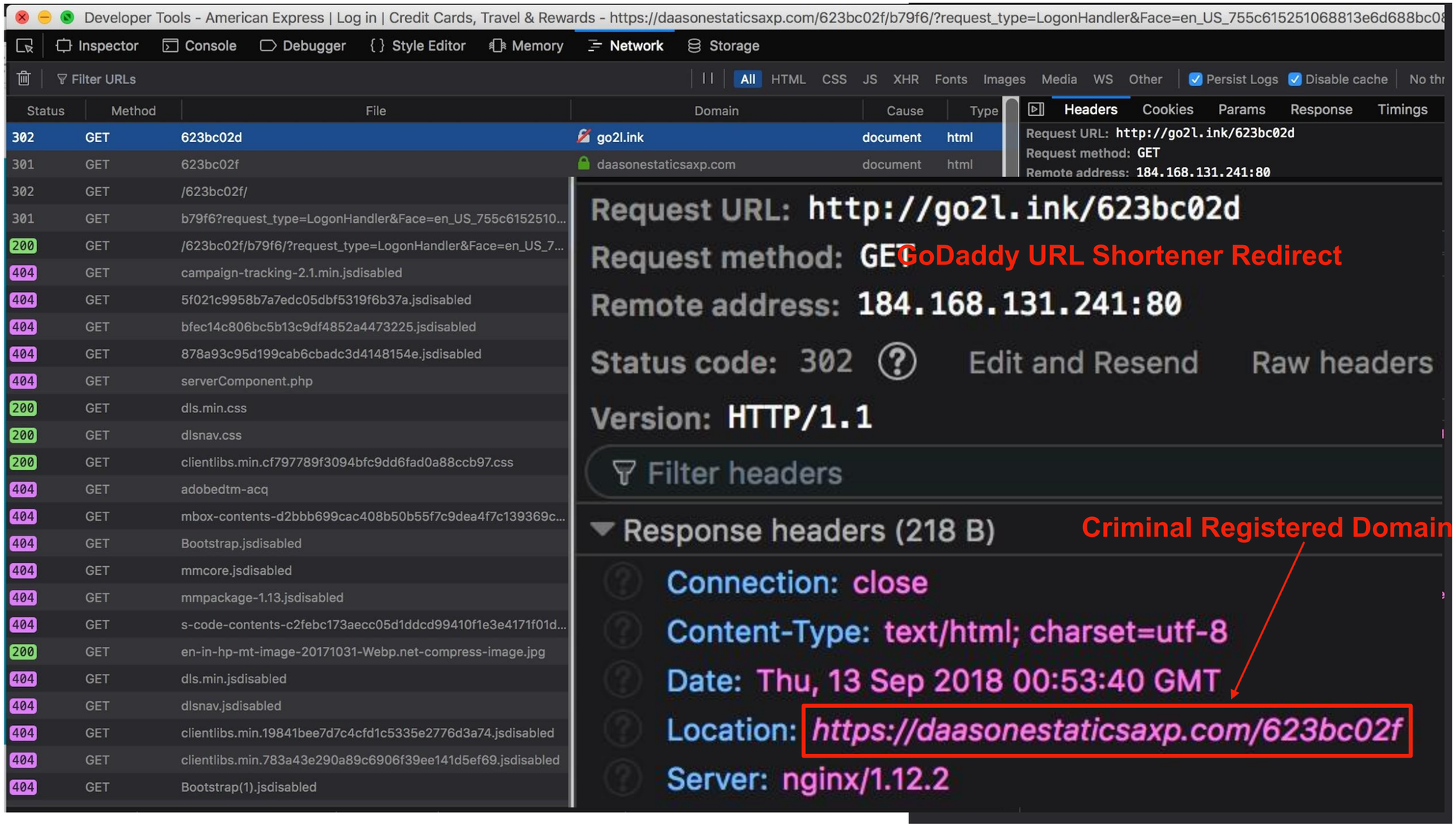
0 / 59

Detection | Details | Community

Ad-Aware	Clean	AegisLab	Clean
AhnLab-V3	Clean	ALYac	Clean
Antiy-AVL	Clean	Arcabit	Clean
Avast	Clean	Avast Mobile Security	Clean
AVG	Clean	Avira	Clean
AVware	Clean	Babable	Clean
Baidu	Clean	BitDefender	Clean
Bkav	Clean	CAT-QuickHeal	Clean
ClamAV	Clean	CMC	Clean
Comodo	Clean	Cylance	Clean
Cyren	Clean	DrWeb	Clean
Emsisoft	Clean	eScan	Clean
ESET-NOD32	Clean	F-Prot	Clean
F-Secure	Clean	Fortinet	Clean
GData	Clean	Jiangmin	Clean
K7AntiVirus	Clean	K7GW	Clean
Kaspersky	Clean	Kingsoft	Clean
Malwarebytes	Clean	MAX	Clean
McAfee	Clean	McAfee-GW-Edition	Clean
Microsoft	Clean	NANO-Antivirus	Clean
Panda	Clean	Qihoo-360	Clean
Rising	Clean	SentinelOne	Clean
Sophos AV	Clean	SUPERAntiSpyware	Clean
Symantec	Clean	TACHYON	Clean
Tencent	Clean	*TheHacker*	*Clean*
TrendMicro	Clean	TrendMicro-HouseCall	Clean
VBA32	Clean	VIPRE	Clean
ViRobot	Clean	Yandex	Clean
Zillya	Clean	ZoneAlarm	Clean
Zoner	Clean	Alibaba	Unable to proc
CrowdStrike Falcon	Unable to process file type	Cybereason	Unable to proc
eGambit	Unable to process file type	Endgame	Unable to proc
Palo Alto Networks	Unable to process file type	Sophos ML	Unable to proc
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to proc
Webroot	Unable to process file type		

```
$ cat AMXCORP11092018LETTER.pdf |xxd|grep -iC3 uri

00013430: 3532 2034 3633 2e31 3235 3736 2035 3035  52 463.12576 505
00013440: 2e34 3236 3838 5d0a 2f41 203c 3c2f 5479  .42688]./A <</Ty
00013450: 7065 202f 4163 7469 6f6e 0a2f 5320 2f55  pe /Action./S /U
00013460: 5249 0a2f 5552 4920 2868 7474 703a 2f2f  RI./URI (http://
00013470: 676f 326c 2e69 6e6b 2f36 3233 6263 3032  go2l.ink/623bc02
00013480: 6429 3e3e 3e3e 5d0a 2f43 6f6e 7465 6e74  d)>>>>]./Content
00013490: 7320 3720 3020 520a 2f50 6172 656e 7420  s 7 0 R./Parent
```


Developer Tools - American Express | Log in | Credit Cards, Travel & Rewards - https://daasonestaticsaxp.com/623bc02f/b79f6/?request_type=LogonHandler&Face=en_US_755c615251068813e6d688bc08
Inspector
Console
Debugger
Style Editor
Memory
Network
Storage
Filter URLs
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Persist Logs
Disable cache
Status
Method
File
Domain
Cause
Type
302 GET 623bc02d go2l.ink document html
301 GET 623bc02f daasonestaticsaxp.com document html
302 GET /623bc02f/
301 GET b79f6?request_type=LogonHandler&Face=en_US_755c6152510...
200 GET /623bc02f/b79f6/?request_type=LogonHandler&Face=en_US_7...
404 GET campaign-tracking-2.1.min.jsdisabled
404 GET 5f021c9958b7a7edc05dbf5319f6b37a.jsdisabled
404 GET bfec14c806bc5b13c9df4852a4473225.jsdisabled
404 GET 878a93c95d199cab6cbadc3d4148154e.jsdisabled
404 GET serverComponent.php
200 GET dls.min.css
200 GET dlsnav.css
200 GET clientlibs.min.cf797789f3094bfc9dd6fad0a88ccb97.css
404 GET adobedtm-acq
404 GET mbox-contents-d2bbb699cac408b50b55f7c9dea4f7c139369c...
404 GET Bootstrap.jsdisabled
404 GET mmcore.jsdisabled
404 GET mmpackage-1.13.jsdisabled
404 GET s-code-contents-c2febc173aecc05d1ddcd99410f1e3e4171f01d...
200 GET en-in-hp-mt-image-20171031-Webp.net-compress-image.jpg
404 GET dls.min.jsdisabled
404 GET dlsnav.jsdisabled
404 GET clientlibs.min.19841bee7d7c4cfd1c5335e2776d3a74.jsdisabled
404 GET clientlibs.min.783a43e290a89c6906f39ee141d5ef69.jsdisabled
404 GET Bootstrap(1).jsdisabled
Headers
Cookies
Params
Response
Timings
Request URL: http://go2l.ink/623bc02d
Request method: GET
Remote address: 184.168.131.241:80
Request URL: http://go2l.ink/623bc02d
Request method: GET
GoDaddy URL Shortener Redirect
Remote address: 184.168.131.241:80
Status code: 302
Edit and Resend
Raw headers
Version: HTTP/1.1
Filter headers
Response headers (218 B)
Criminal Registered Domain
Connection: close
Content-Type: text/html; charset=utf-8
Date: Thu, 13 Sep 2018 00:53:40 GMT
Location: https://daasonestaticsaxp.com/623bc02f
Server: nginx/1.12.2

American Express | Log in | Cre

https://daasonestaticsaxp.com/623bc02f/0fecd/?request_type=LogonHandler&Face=en_

Search

My Account | Cards | Travel | Insurance | Rewards | Business | Contact Us | Log In

User ID

PASSWORD

Password

Remember Me

Log In

Forgot your User ID or Password?

Register for Online Services

Let your friends pay for what you love!

Refer the American Express® Card to your friends and earn up to Rs.20,000 Cash Credit*

Refer Now

*Terms & Conditions apply.

Pay Your Card Bill

Download Mobile App

Apply for a Supplementary Card

Latest Offers and Updates from American Express

American Express Referral Campaign

Samsung Pay

Registration Whois Datapoints

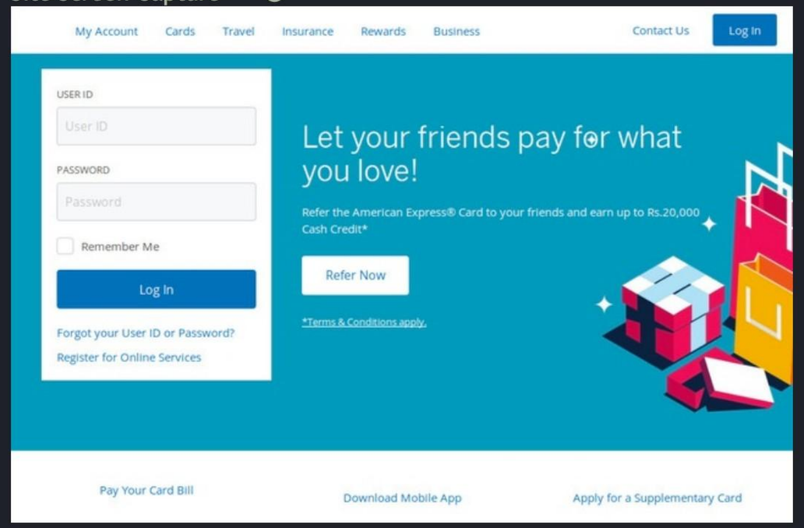
Registrar:	GoDaddy.com, LLC
Creation Date:	2018-08-04T13:38:33.000Z
Email:	Select Contact Domain Holder link at https: Select Contact Domain Holder link at https:
Status:	clientTransferProhibited
Name Servers:	NS53.DOMAINCONTROL.COM

Netblock Whois Datapoints

Country:	SG
RIR:	APNIC
Creation Date:	2016-09-13
Owner Name:	Leaseweb Asia Pacific pte. ltd.
Status:	unknown
ASN:	AS59253 (rank)

Current Live DNS Resolution

Site Screen Capture



Zetalytics DNS History

Domain	Date	IP
www.aexp-statics.org	2018-09-12	209.58.178.43
merchant-suppliesamericanexpress...	2018-09-11	209.58.178.43
merchant-suppliesamericanexpress...	2018-09-11	209.58.178.43
www.dietischlerei.net	2018-09-05	209.58.178.43
mail.dietischlerei.net	2018-09-04	209.58.178.43
cpanel.dietischlerei.net	2018-09-04	209.58.178.43
www.daasonestaticsaxp.com	2018-09-01	209.58.178.43
dietischlerei.net	2018-08-31	209.58.178.43
american365express.info	2018-08-30	209.58.178.43
american365express.org	2018-08-29	209.58.178.43
american365express.net	2018-08-29	209.58.178.43
daasonestaticsaxp.com	2018-08-21	209.58.178.43
www.aexp-statics.com	2018-08-11	209.58.178.43
amexamericanexpress.com	2018-08-10	209.58.178.43
ns1.jack404.id	2018-08-08	209.58.178.43
aexp-statics.com	2018-08-08	209.58.178.43

bit.ly/2022zc

Go to www.menti.com and use the code 67 29 15 3

WHAT ELSE WERE YOU HOPING TO GET OUT OF THIS SESSION?

Mentimeter

Press ENTER to pause scroll

Press s to hide image

HANDS-ON WITH HOMOGLYPHS

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

1 500

Fraud Domain ☑ has ns	Victim Domain		Timestamp	Link	Priority	Rank
liverpoolrnuseums.org.uk	liverpoolmuseums.org.uk	(US)	2018-09-12 04:50	UK	0	118037
childcarre.co.uk	childcare.co.uk	(IE)	2018-09-12 03:29	UK	0	174098
aviva-popett.uk	aviva-popet.uk	(US)	2018-09-12 15:04	UK	0	
duuno.co.uk	duno.co.uk	(DE)	2018-09-12 14:53	UK	0	
svvannlighting.co.uk	swannlighting.co.uk	(GB)	2018-09-12 12:21	UK	0	
popettaviva.co.uk	popetaviva.co.uk	(US)	2018-09-12 06:16	UK	0	
gfholdlng.co.uk	gfholding.co.uk	(DE)	2018-09-12 04:11	UK	0	
alumascvvms.co.uk	alumascwms.co.uk	(GB)	2018-09-12 03:57	UK	0	
prrospot.co.uk	prospot.co.uk	(GB)	2018-09-12 02:24	UK	0	
mmwjones.co.uk	mwjones.co.uk	(DE)	2018-09-11 05:46	UK	0	
apllusgroup.co.uk	aplusgroup.co.uk	(GB)	2018-09-11 00:52	UK	0	
hcpp.co.uk	hcp.co.uk	(GB)	2018-09-11 00:11	UK	0	
classscharts.com	classcharts.com	(US)	2018-09-10 17:03	UK	0	118707
thegrandcaffe.co.uk	thegrandcafe.co.uk	(GB)	2018-09-10 23:08	UK	0	
gaadirect.co.uk	gadirect.co.uk	(GB)	2018-09-10 01:01	UK	0	
jbbpm.co.uk	jbpm.co.uk	(GB)	2018-09-10 01:00	UK	0	
havvk-group.co.uk	hawk-group.co.uk	(US)	2018-09-10 00:30	UK	0	
barclayss.com	barclays.com	(US)	2018-09-09 16:53	UK	0	28805
hbbhonline.co.uk	hbhonline.co.uk	(GB)	2018-09-09 21:40	UK	0	
accomplish-group.co.uk	accomplish-group.co.uk	(GB)	2018-09-09 13:06	UK	0	
cootb.co.uk	cotb.co.uk	(GB)	2018-09-09 12:02	UK	0	

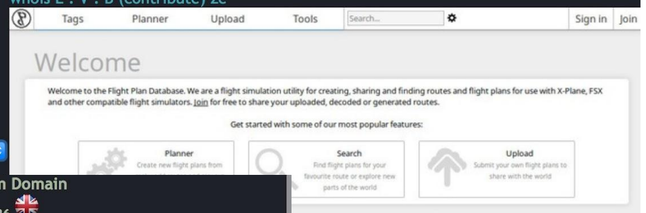
fligtplandatabase.com

whois E . V . B (contribute) zc
2018-07-25 21:23:41 -0400

alt interface

flightplandatabase.com

google (with site:) HQ
whois E . V . B (contribute) zc



Potential Fraud Domain

Priority
0
Categorize

UK

Potential Victim Domain

51.140.122.226

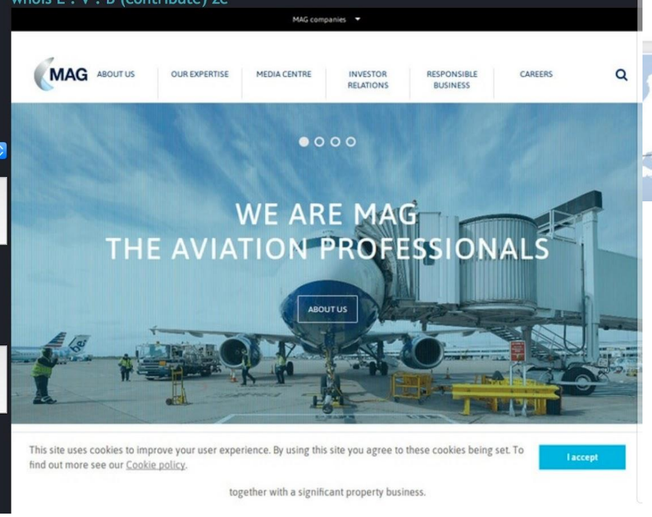
magalrports.com

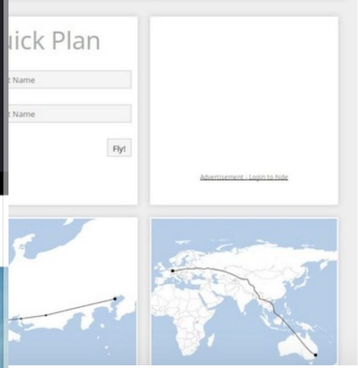
whois E . V . B (contribute) zc
2018-07-25 16:03:00 -0400

alt interface

magairports.com

google (with site:) HQ
whois E . V . B (contribute) zc





Confirm

Pass


Potential Fraud Domain
Priority
0
Categorize
vvyedean.com
whois E . V . B (contribute) zc
2018-07-26 06:24:50 -0400
alt interface
Police / Military Uniforms
Potential Victim Domain
62.233.121.42
wyedean.com
google (with site:) HQ
whois E . V . B (contribute) zc
Wyedean
HOME
OUR STORY
SERVICES
PRODUCTS
THE TEAM
GALLERY
SHOP
BLOG
FAQS
CONTACT
WYEDEAN
Manufacturers of uniforms, braid and accoutreme
n - More than just a developer
turer of military uniforms, braid, insignia, regalia and accoutrement.
Potential Fraud Domain
Priority
0
Categorize
goodwingruop.com
whois E . V . B (contribute) zc
2018-07-25 16:54:11 -0400
alt interface
Potential Victim Domain
212.57.250.136
goodwingroup.com
google (with site:) HQ
whois E . V . B (contribute) zc
GOODWIN PLC
Established 1883
Mechanical Engineering
Goodwin International Limited
Goodwin Steel Castings Limited
Easat Radar Systems Limited
Internet Central Limited
Noreva GmbH
Goodwin Pumps India Private Limited
Goodwin Shanghai Co. Limited
Goodwin (Shanxi) Pump Company Ltd
Goodwin Korea Co. Limited
Goodwin Valve and Pump Co. Ltd
Refractory Engineering
Dupré Minerals Limited
Goodwin Refractory Services Limited
Hoben International Limited
Sandersfire International
Gold Star Powders India Private Ltd
Siam Casting Powders Limited
Ultratec Jewelry Supplies Limited
SRS (QingDao) Casting Materials Company Limited
Gold Star Brazil Limited
Share Price: £18.60
Change of £+0.10
at 15:47 on 25-07-2018
Information for INVESTORS click here
GOODWIN apprentice opportunities
London Stock Exchange
PREMIUM LISTED
GOODWIN VALVES, PUMPS AND CASTINGS
This website uses cookies to personalize your user experience and to study how our website is being used. You consent to our cookies if you continue to use this website.
Allow all cookies
Use necessary cookies only
UK
Confirm
Pass
Easat Radar Systems

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Passive (Aggressive) DNS

USE CASE: FOOTPRINTING

RSAC.COM

Reliance Steel and Aluminum

Uncover activity related to:

rsac.com

Search domain data

is an authoritative NS

Uncover activity related to:

Valid CIDR list:
64.94.109.64/26
64.94.96.0/20
64.94.109.64/32
64.94.109.64/31
64.94.109.64/30
64.94.109.64/29
64.94.109.64/28
64.94.109.64/27
64.94.109.64/26
64.94.109.0/25
64.94.109.0/24
64.94.108.0/23
64.94.108.0/22
64.94.104.0/21
64.94.96.0/20
64.94.96.0/19
64.94.64.0/18
64.94.0.0/17
64.94.0.0/16

/ 26

Set domain tagging entity type: tag

conglomerate × producer × aluminum × steel × aerospace × energy ×

Type to add tags for ...

+ rsac.com

Set IP tagging ent

Type to add tags for ...

+ 64.94.109.64/26

Show	Source	Records	Status
☑ ○	**Zetalytics Hostname History**	1984	278 ms
☑ ○	Malware DNS Activity	0	548 ms
☑ ○	Registration Whois	1	81 ms
☐ ○	with same email		
☑ ○	Live DNS	8	405 ms
☑ ○	NS glue history	0	392 ms
☑ ○	a-passive	3	194 ms
☑ ○	Authoritative NS	270	1381 ms
☑ ○	Site screen capture	0	

Show	Source	Records	Status
☑ ○	**Zetalytics Passive DNS**	34	1764 ms
☑ ○	Malware DNS Activity	0	1319 ms
☑ ○	Netblock whois	1	16682 ms
☐ ○	with same email		
☑ ○	Reverse DNS	3	1125 ms
☑ ○	a-passive	0	1079 ms
☐ ○	cn-passive-ips		Click 2 Run
☑ ○	Auth NS Glue	0	1061 ms
☐ ○	Tor Exit Nodes	0	540 ms

Registration Whois Datapoints

Registrar:	Network Solutions, LLC.
Creation Date:	1997-03-08T05:00:00.000Z
Status:	clientTransferProhibited
Name Servers:	SNOOPY.RSAC.COM

Netblock Whois Datapoints

Country:	US
RIR:	ARIN
Creation Date:	2000-06-05
Owner Name:	Reliance Steel & Aluminum Co
Status:	reassignment

Authoritative NS

Domains Served By Name Server

customfabco.com
lbi-metals.com
liebovichwisc.com
liebovichiowa.com
liebovichsteel.com
hagertysteel.com
goodmetals.com
metalsrockford.com
liebovich.com
smithpipe.com
claytonmetals.com
precisionflamecuttingandsteel.com
precisionflamecutting.com
pflame.com
rmapmetals.com
emjmetals.info
www.nsalloys.com
altair-co.com
trident-metals.com
findareliancerewardsmedicalprovider.com
centralplainssteel.net
jorgensensteel.org
cccsteel.net
bac1490.com
terms-conditions.net
emjmedals.com
reliancerewardsmedicalprovider.com
emjmedals.org
reliancesteelunioncity.com
reliancerewardsmedicalproviders.com
centralplainssteelwichita.com
rsacfamily.net

Registration Whois Datapoints

Registrar:	Network Solutions, LLC.
Creation Date:	1997-03-08T05:00:00.000Z
Status:	clientTransferProhibited
Name Servers:	SNOOPY.RSAC.COM

Current Live DNS Resolution

rsac.com	A	198.72.80.37
snoopy.rsac.com	A	209.10.101.67
snoopy.rsac.com	A	64.94.109.67
mx1.rsac.iphmx.com	A	68.232.131.81
mx1.rsac.iphmx.com	A	68.232.137.96
mx1.rsac.iphmx.com	A	68.232.142.172
mx1.rsac.iphmx.com	A	68.232.148.75
woodstock.rsac.com	A	72.44.207.193
rsac.com	MX	mx1.rsac.iphmx.com
rsac.com	MX	mx2.rsac.iphmx.com

Show More

Uncover activity related to:

Valid CIDR list:
198.72.80.0/20
198.72.80.0/24
198.72.80.37/32
198.72.80.36/31
198.72.80.36/30
198.72.80.32/29
198.72.80.32/28
198.72.80.32/27
198.72.80.0/26
198.72.80.0/25
198.72.80.0/24
198.72.80.0/23
198.72.80.0/22
198.72.80.0/21
198.72.80.0/20
198.72.64.0/19
198.72.64.0/18
198.72.0.0/17
198.72.0.0/16

/ 32

Set IP tagging ent

Type to add tags for ...

+ 198.72.80.37/32

Show	Source	Records	Status
☑	Zetalytics Passive DNS	184	1595 ms
☑	Malware DNS Activity	0	650 ms
☑	Netblock whois	1	469 ms
☐	with same email		
☑	Reverse DNS	1	855 ms
☑	a-passive	0	329 ms
☐	cn-passive-ips		Click 2 Run
☑	Auth NS Glue	0	386 ms
☐	Tor Exit Nodes	0	470 ms

Netblock Whois Datapoints

Country:	US
RIR:	ARIN
Creation Date:	2012-08-20 2018-06-23
Owner Name:	Network Redux LLC
Email:	hostmaster@networkredux.com | abuse@netw...
Status:	allocation
ASN:	AS14744 (rank)
PTR:	evs.rsac.com

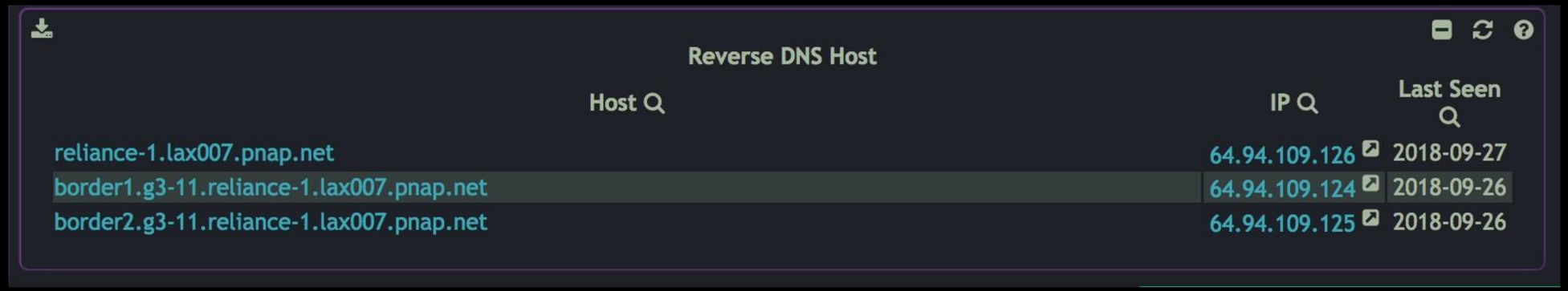
Zetalytics DNS History

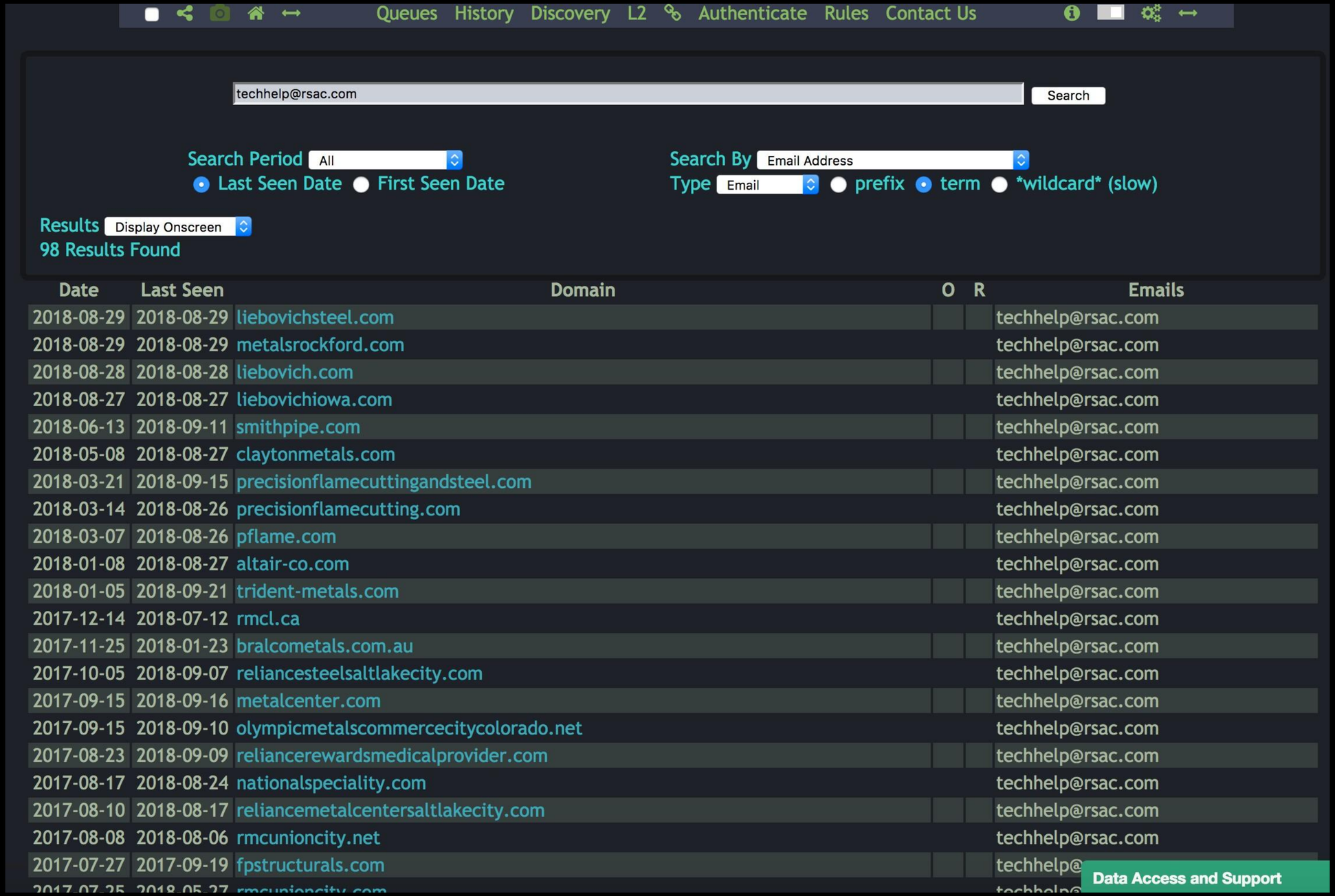
Domain	Date	IP
liebovich.com	2018-08-28	198.72.80.37
liebovichsteel.com	2018-08-28	198.72.80.37
liebovichwisc.com	2018-08-28	198.72.80.37
goodmetals.com	2018-08-28	198.72.80.37
hagertysteel.com	2018-08-28	198.72.80.37
liebovichiowa.com	2018-08-28	198.72.80.37
www.smithpipe.com	2018-06-15	198.72.80.37
smithpipe.com	2018-06-07	198.72.80.37
www.trident-metals.com	2018-05-30	198.72.80.37
trident-metals.com	2018-05-29	198.72.80.37
www.foxmetals.com	2018-04-16	198.72.80.37
foxmetals.com	2018-03-03	198.72.80.37
lampros.com	2018-02-14	198.72.80.37
lamprossteel.com	2018-01-27	198.72.80.37
american-steel.com	2018-01-26	198.72.80.37
www.lamprossteel.com	2018-01-26	198.72.80.37
www.american-metals.com	2018-01-26	198.72.80.37
www.american-steel.com	2018-01-26	198.72.80.37
american-metals.com	2018-01-26	198.72.80.37
www.jorgensensteel.com	2017-12-18	198.72.80.37
jorgensensteel.com	2017-12-16	198.72.80.37
wordpress1.rsac.com	2017-11-30	198.72.80.37
ftp.phoenixmetals.com	2017-11-09	198.72.80.37
www.rsac-corp.com	2017-08-01	198.72.80.37

Zetalytics DNS History

Domain	Date	IP
dr.rsacdev.com	2018-06-08	64.94.109.85
cv2.emjmetals.com	2017-02-13	64.94.109.122
h.18.cofile.net	2016-09-25	64.94.109.125
direct.hillsdale.net	2016-09-14	64.94.109.71
h.04.cofile.net	2016-08-15	64.94.109.119
h.06.cofile.net	2016-08-15	64.94.109.121
s4273x.pbxtra.fonality.com	2016-07-22	64.94.109.117
h.13.cofile.net	2016-07-22	64.94.109.115
h.11.cofile.net	2016-07-21	64.94.109.71
g.14.cofile.net	2016-05-16	64.94.109.125
g.02.cofile.net	2016-05-16	64.94.109.125
lsan-gate.rsac.com	2015-11-21	64.94.109.117
www.varsteel.com	2015-10-11	64.94.109.72
exchange.rsac.com	2015-09-27	64.94.109.116
hal.rsac.com	2015-09-26	64.94.109.66
www.rsmetals.com	2015-09-03	64.94.109.72
www.rsac-corp.com	2015-09-03	64.94.109.72
forum.rsac.com	2015-08-30	64.94.109.69
vpn.rsac.com	2015-08-30	64.94.109.123
0a44410413bd770f9ac910c5238b14f...	2015-06-21	64.94.109.87
helpdesk.rsac.com	2015-05-20	64.94.109.69
test.rsac.com	2015-05-04	64.94.109.68
topekadirect.cjonline.com	2015-04-07	64.94.109.71
snoopy.rsac.com	2015-02-25	64.94.109.67
www.15-5.com	2015-01-30	64.94.109.72
15-5.com	2014-09-25	64.94.109.72
rsac-test.com	2014-09-23	64.94.109.72
centralplainssteel.com	2014-09-11	64.94.109.72
rsmetals.com	2014-09-10	64.94.109.72
rsac-corp.com	2014-09-07	64.94.109.72
bralcosw.com	2014-09-02	64.94.109.72
varsteel.com	2014-08-27	64.94.109.72
centralplainssteelco.com	2014-08-25	64.94.109.72

Show Less


Reverse DNS Host
Host
IP
Last Seen
reliance-1.lax007.pnap.net
64.94.109.126
2018-09-27
border1.g3-11.reliance-1.lax007.pnap.net
64.94.109.124
2018-09-26
border2.g3-11.reliance-1.lax007.pnap.net
64.94.109.125
2018-09-26


Queues History Discovery L2 Authenticate Rules Contact Us
techhelp@rsac.com
Search
Search Period All
Last Seen Date First Seen Date
Search By Email Address
Type Email prefix term *wildcard* (slow)
Results Display Onscreen
98 Results Found
Date Last Seen Domain O R Emails
2018-08-29 2018-08-29 liebovichsteel.com techhelp@rsac.com
2018-08-29 2018-08-29 metalsrockford.com techhelp@rsac.com
2018-08-28 2018-08-28 liebovich.com techhelp@rsac.com
2018-08-27 2018-08-27 liebovichiowa.com techhelp@rsac.com
2018-06-13 2018-09-11 smithpipe.com techhelp@rsac.com
2018-05-08 2018-08-27 claytonmetals.com techhelp@rsac.com
2018-03-21 2018-09-15 precisionflamecuttingandsteel.com techhelp@rsac.com
2018-03-14 2018-08-26 precisionflamecutting.com techhelp@rsac.com
2018-03-07 2018-08-26 pflame.com techhelp@rsac.com
2018-01-08 2018-08-27 altair-co.com techhelp@rsac.com
2018-01-05 2018-09-21 trident-metals.com techhelp@rsac.com
2017-12-14 2018-07-12 rmcl.ca techhelp@rsac.com
2017-11-25 2018-01-23 bralcometals.com.au techhelp@rsac.com
2017-10-05 2018-09-07 reliancesteelsaltlakecity.com techhelp@rsac.com
2017-09-15 2018-09-16 metalcenter.com techhelp@rsac.com
2017-09-15 2018-09-10 olympicmetalscommercecitycolorado.net techhelp@rsac.com
2017-08-23 2018-09-09 reliancerewardsmedicalprovider.com techhelp@rsac.com
2017-08-17 2018-08-24 nationalspeciality.com techhelp@rsac.com
2017-08-10 2018-08-17 reliancemetalcentersaltlakecity.com techhelp@rsac.com
2017-08-08 2018-08-06 rmcunioncity.net techhelp@rsac.com
2017-07-27 2017-09-19 fpstructurals.com techhelp@
Data Access and Support

Registration Whois Datapoints

Registrar:	Network Solutions, LLC.
Creation Date:	1997-03-08T05:00:00.000Z
Status:	clientTransferProhibited
Name Servers:	SNOOPY.RSAC.COM

Current Live DNS Resolution

rsac.com	A	198.72.80.37
snoopy.rsac.com	A	209.10.101.67
snoopy.rsac.com	A	64.94.109.67
mx1.rsac.iphmx.com	A	68.232.131.81
mx1.rsac.iphmx.com	A	68.232.137.96
mx1.rsac.iphmx.com	A	68.232.142.172
mx1.rsac.iphmx.com	A	68.232.148.75
woodstock.rsac.com	A	72.44.207.193
rsac.com	MX	mx1.rsac.iphmx.com
rsac.com	MX	mx2.rsac.iphmx.com

Show More

Filter... x

v1

- cname2qname
- domain2aaaa
- domain2cname
- domain2ip
- domain2malwaredns
- domain2malwarehttp
- domain2mx
- domain2ns
- domain2ptr
- domain2txt
- domain2whois
- email_address
- email_domain
- email_user
- hash2malwaredns
- hash2malwarehttp
- hostname
- ip
- ip2malwaredns
- **mx2domain**
- ns2domain

Send a Sample Request

https://zonecruncher.com/api/v1/mx2domain url

Parameters

Parameter

q	mx1.rsac.iphmx.com	String
toBaseDomain	toBaseDomain	Boolean
token	PUTYOURTOKENHERE	String
start	start	
end	end	
tsfield	tsfield	String

Send

Response

X


```
{
    "info": "52 results found.",
    "total": 52,
    "returning": 52,
    "results": [
        {
            "domain": "tomametals.com",
            "qname": "tomametals.com",
            "qtype": "15",
            "date": "2016-04-06",
            "last_seen": "2017-09-29",
            "type": "mx",
            "value": "mx1.rsac.iphmx.com"
        },
        {
            "domain": "nsalloys.com",
            "qname": "www.nsalloys.com",
            "qtype": "15",
            "date": "2018-07-05",
            "last_seen": "2018-07-05",
            "type": "mx",
            "value": "mx1.rsac.iphmx.com"
        },
        {
            "domain": "customfabco.com",
```

CAUTIONARY TALES

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- You are the product
- Who are you signalling?
- What can be forged? (untrusted data)
- Nation State Interests
- Corporate Interests vs Public Interest

YOU ARE THE PRODUCT

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- 1.1.1.1, 8.8.8.8, 9.9.9.9,
- 101.101.101.101,
  114.114.114.114
- Someone is recording your DNS lookups
- Who gains access?
- What countries gain access to your DNS lookups?
- For what purposes?
- Re-sold to marketers?
- Correlation with other tracking mechanisms?

Go to www.menti.com and use the code 67 29 15 3

GO TO http://sink.glass/

Mentimeter

Find your Recursive Resolver IP, copy and paste it here. If you know your usual preferred resolver, you can also paste it here, such as 4.2.2.2:

Press s to hide image

RESOURCES & NEXT STEPS:

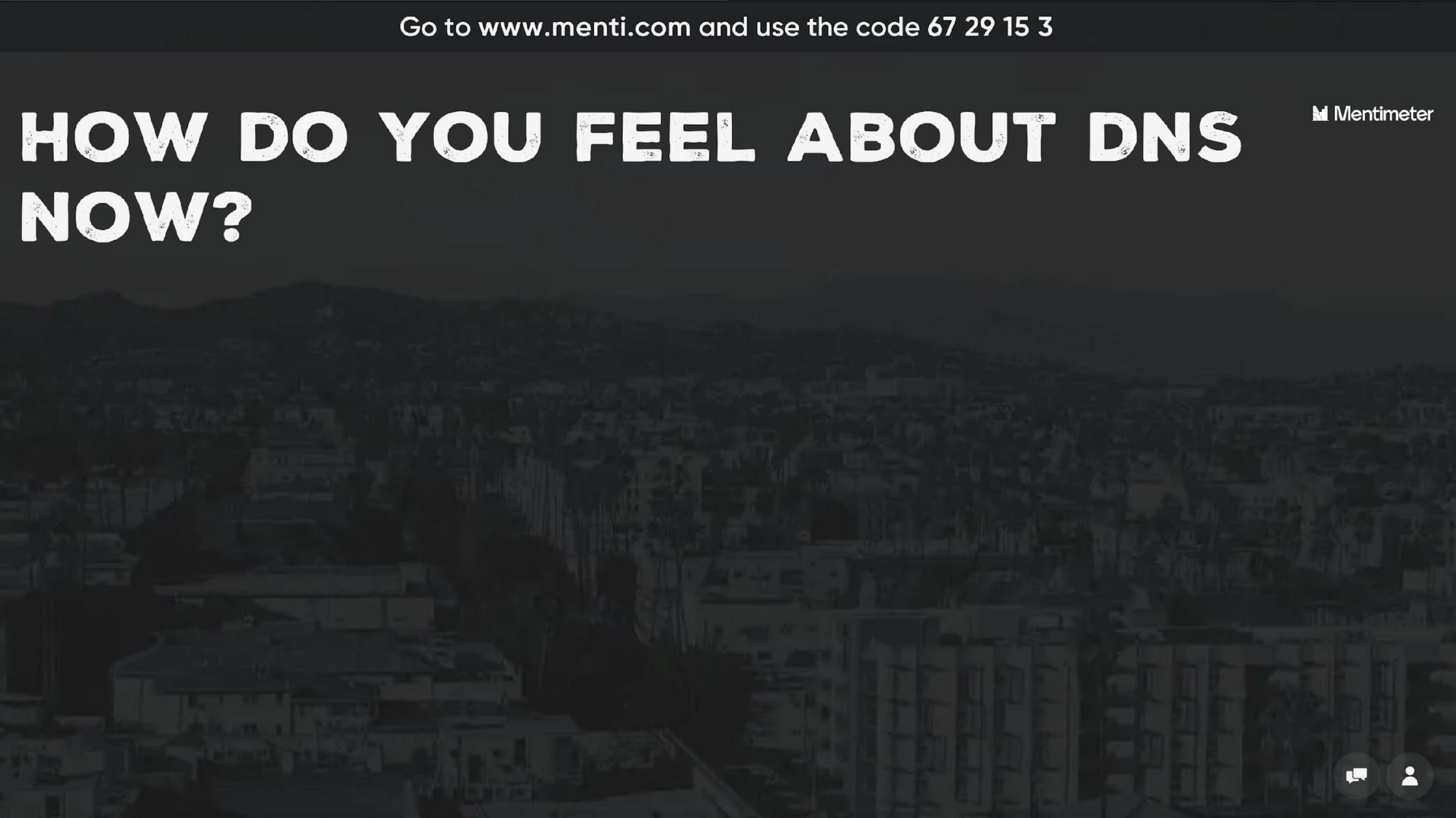
M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- IANA.org DNS Parameters
- What recursive resolver am I using? http://sink.glass/
- VPNs that don't route your DNS traffic
- DNS Privacy Efforts
- Free passive DNS accounts to sign up for
- Recommended reading list

Questions? April Lorenzen april@Zetalytics.com

Go to www.menti.com and use the code 67 29 15 3

HOW DO YOU FEEL ABOUT DNS NOW?



April Lorenzen data@dissectcyber.com

Contact

For additional questions, please email:

training_committee-chair@mailman.m3aawg.org