



Proton Pivots

BITE-SIZE EXERCISE

Expanding on ProtonMail spoof domains

APRIL LORENZEN
Chief Data Scientist
[@zetalytics.com](https://twitter.com/zetalytics.com)

ZETAlytics

million

Argentina
Bolivia
Brazil
Chile
Colombia
Ecuador
Falkland Islands
French Guiana
Guyana
Paraguay
Peru
Suriname
Uruguay
Venezuela

111.3 billion

Anguilla, Antigua And Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, Bonaire, Saint Eustatius And Saba, Canada, Cayman Islands, Costa Rica, Cuba, Curacao, Dominica, Dominican Republic, El Salvador, Greenland, Grenada, Guadeloupe, Guatemala, Haiti, Honduras, Jamaica, Martinique, Mexico, Montserrat, Netherlands Antilles, Nicaragua, Panama, Puerto Rico, Saint Barthelemy, Saint Kitts And Nevis, Saint Lucia, Saint Martin, Saint Pierre And Miquelon, Saint Vincent And The Grenadines, Sint Maarten, Trinidad And Tobago, Turks And Caicos Islands, United States, United States Minor Outlying Islands, Virgin Islands

17.3 billion

Aland Islands, Albania, Andorra, Austria, Belarus, Belgium, Bosnia

15.8 billion

AGENDA

- Analyze each indicator in ThreatConnect's excellent blog post
- Utilize Zetalytics larger collection of geo-diverse passive DNS
- Find and share more clues:
 - Attribution work
 - Network protection
 - Unrelated groups targeting ProtonMail users

Tool suite: ZoneCruncher with Zetalytics Passive DNS

248 million

Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo - Brazzaville, Congo, The Democratic Republic Of The Congo, Cote D'Ivoire, Djibouti, Egypt, Equatorial Guinea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-bissau, Kenya, Lesotho, Liberia, Libya, Arab Jamahiriya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Mayotte, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Saint Helena, Sao Tome And Principe, Senegal, Seychelles, Sierra Leone, South Africa, South Sudan, Sudan, Swaziland, Tanzania, United Republic Of, Togo, Tunisia, Uganda, Western Sahara, Zambia, Zimbabwe

636 million

American Samoa, Asia Pacific Region, Australia, Cook Islands, Fiji, French Polynesia, Guam, Kiribati, Marshall Islands, Micronesia, Federated States Of, Nauru, New Caledonia, New Zealand, Niue, Norfolk Island, Northern Mariana Islands, Palau, Papua New Guinea, Pitcairn, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis And Futuna Islands

protonmail[.]sh

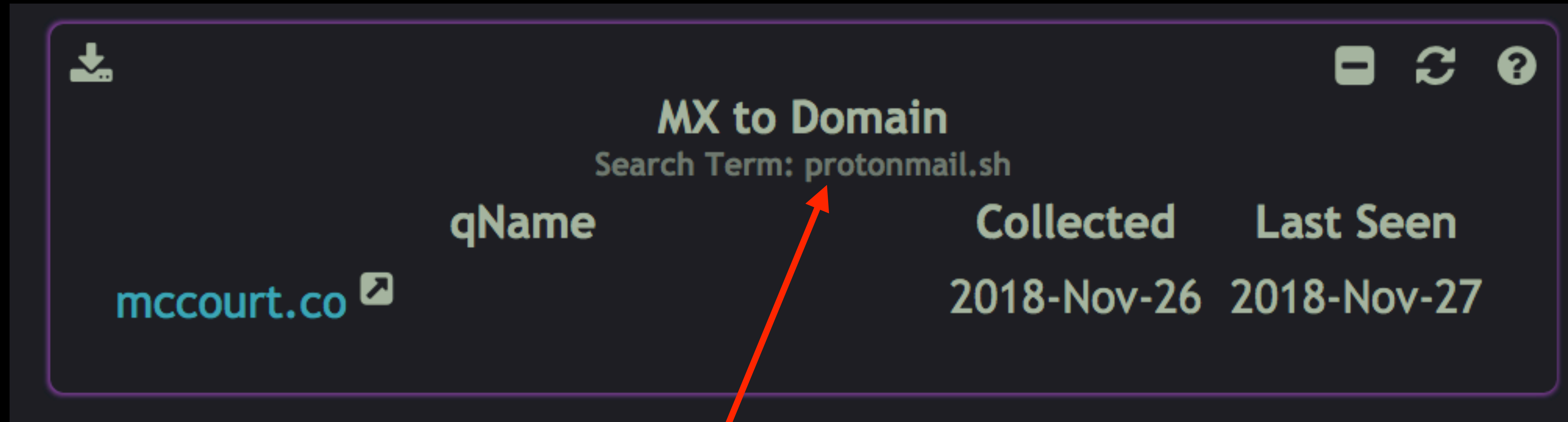
- Identified as definitely part of the phishing attack targeting BellingCat
- mail[.]protonmail[.]sh/password
- mail[.]protonmail[.]sh/keys
forward to
mailprotonmail[.]ch/keys

Tool suite: ZoneCruncher with Zetalytics Passive DNS


2019-05-21 mailsec.protonmail.sh

- Zetalytics passive DNS knows of an additional subdomain, observed on one day only
- **Speculation:** planning phase of attack. Later attacker decides to use subdomain “mail” instead of “mailsec”
- Or could have been part of another, so far undiscovered, narrowly focused attack
- Implications of the A record (an IPv4) could easily be mis-interpreted, so we will not broadcast it publicly at this time

MX RECORD PIVOT



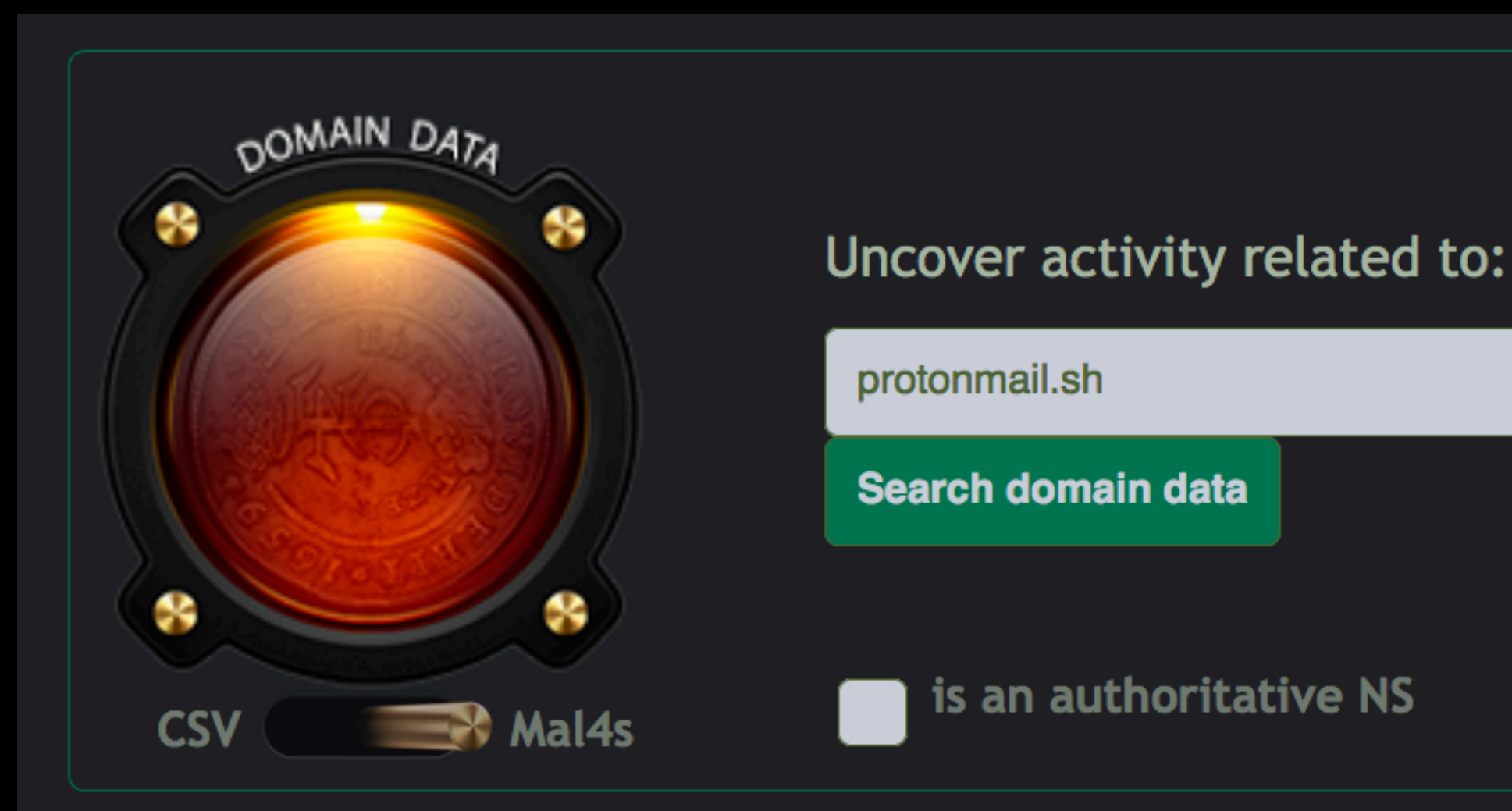
The screenshot shows the 'MX to Domain' search results in ZoneCruncher. The search term is 'protonmail.sh'. The results table has columns for 'qName', 'Collected', and 'Last Seen'. A red arrow points from the 'qName' column to the text 'Searching in ZoneCruncher for protonmail[.]sh automatically performs multiple pivots, providing you with the results on one pane of glass.'

qName	Collected	Last Seen
mccourt.co 	2018-Nov-26	2018-Nov-27

Searching in ZoneCruncher for protonmail[.]sh automatically performs multiple pivots, providing you with the results on one pane of glass.

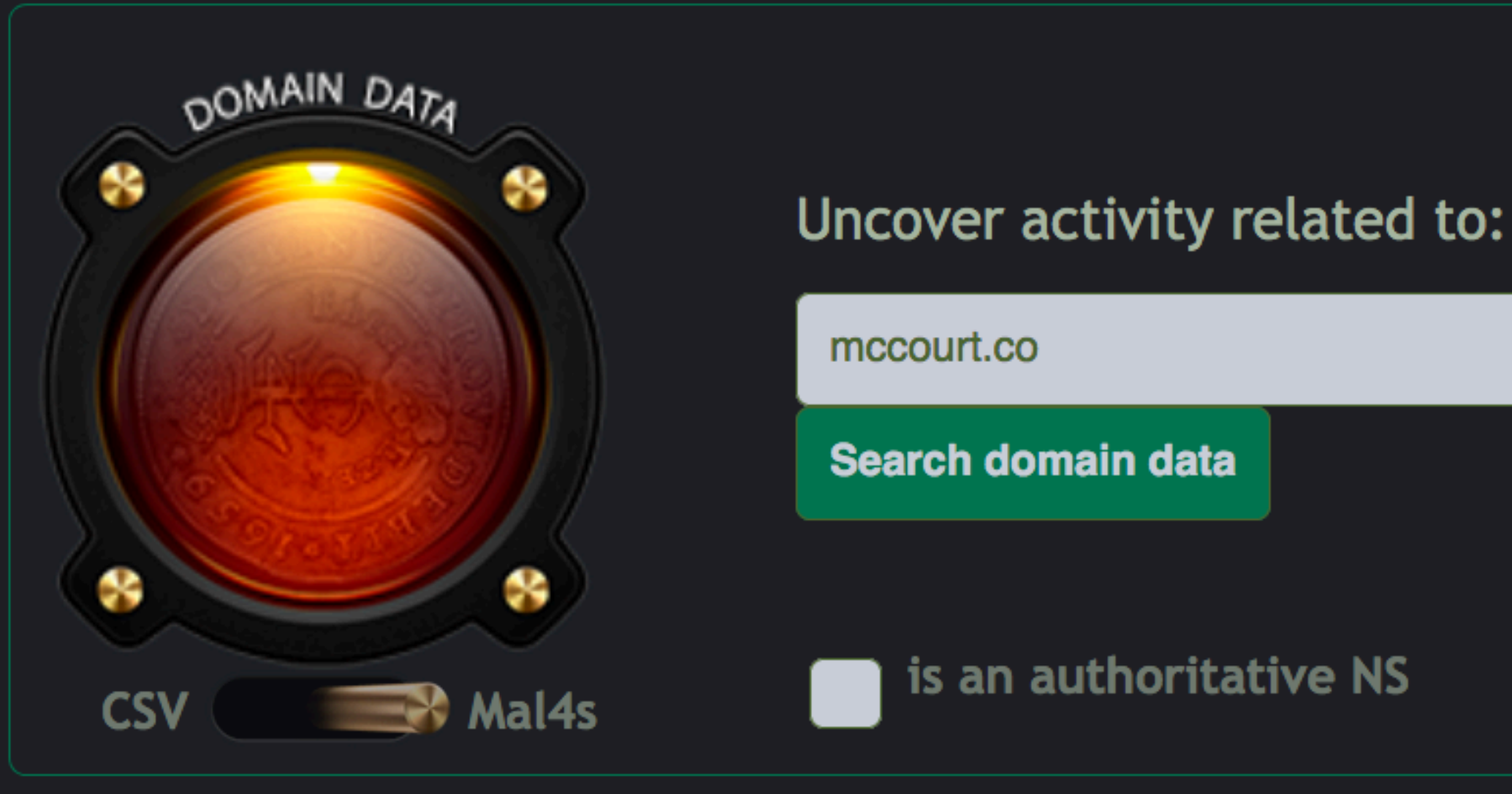
Here we see an unexpected clue, possibly of use in attribution or indicative of a past operation that targeted ProtonMail users.

For just one day at the point of domain registration, mccourt[.]co pointed to protonmail[.]sh for Mail eXchanger aka MX record service. Mail addressed to [user]@mccourt[.]co would PASS THROUGH an inbound SMTP server based on protonmail[.]sh



Same pivot techniques work in ZoneCruncher web portal, scripted JSON API or Maltego transforms

FASCINATING MX RECORDS CHRONOLOGY: MCCOURT[.]CO



WOW - so the very next day after mccourt[.]co points MX record to mail[.]protonmail[.]sh - it then switches to the REAL protonmail[.]ch MX hosts, gets verified with ProtonMail via TXT records, gets real SPF records and - hey that's handy - a DMARC reporting email address :)

pnjmcco@gmail.com

SPECULATION: setup and testing of MitMX (Man in the Mail eXchanger)

2018-11-30	_dmarc.mccourt.co	4v=DMARC1; p=quarantine; rua=mailto:pnjmcco@gmail.com
2018-11-28	mccourt.co)v=spf1 include:_spf.protonmail.ch mx ~all
2018-11-27	mccourt.co	Dprotonmail-verification=63a68fcdf63bf5ecc8b9c4a890daef402e9d0509
2018-11-27	mccourt.co	@protonmail- verification=1c0b3b844b904bc3968e4cc81c9a36c35c7da4cb
2018-11-27	mccourt.co	mailsec.protonmail.ch
2018-11-27	mccourt.co	mail.protonmail.ch
2018-11-26	mccourt.co	mail.protonmail.sh

Same pivot techniques work in ZoneCruncher web portal, scripted JSON API or Maltego transforms

MUCH MORE TO BE SEEN FROM ZETALYTICS PASSIVE DNS

2018-11-26	mccourt.co	mail.protonmail.sh
2018-07-12	www.mccourt.co	209.200.154.51
2018-06-02	mccourt.co	dns1.name-services.com
2018-06-02	mccourt.co	info @ name-services.com
2018-06-02	mccourt.co	209.200.154.51
2018-06-02	mccourt.co	dns2.name-services.com
2018-06-02	mccourt.co	dns4.name-services.com
2018-06-02	mccourt.co	dns3.name-services.com
2018-06-02	mccourt.co	dns5.name-services.com
2018-05-19	mccourt.co	reg-pr-web-suspensionpages-go-co-1680484254.us-east-1.elb.amazonaws.com
2018-05-19	mccourt.co	pr-co-suspensions.go.co
2018-05-19	mccourt.co	52.5.149.42
2018-05-19	mccourt.co	54.164.250.80
2018-05-17	www.mccourt.co	pr-co-suspensions.go.co
2018-05-17	www.mccourt.co	reg-pr-web-suspensionpages-go-co-1680484254.us-east-1.elb.amazonaws.com

2018-04-26	mail.mccourt.co	ghs.googlehosted.com
2018-04-14	mccourt.co	alt3.aspmx.l.google.com
2018-04-14	mccourt.co	alt1.aspmx.l.google.com
2018-04-14	mccourt.co	alt2.aspmx.l.google.com
2018-04-14	mccourt.co	alt4.aspmx.l.google.com
2017-11-25	mccourt.co	ns1.dreamhost.com
2017-11-25	mccourt.co	hostmaster @ dreamhost.com
2017-11-25	mccourt.co	aspmx.l.google.com
2017-11-25	mccourt.co	64.111.110.185
2017-11-25	mccourt.co	ns2.dreamhost.com
2017-01-11	mccourt.co	ns3.dreamhost.com
2016-08-09	www.mccourt.co	64.111.110.185
2015-05-29	www.mccourt.co	mccourt.co
2015-05-29	www.mccourt.co	89.145.89.31
2015-05-13	mccourt.co	mccourt.co
2015-05-13	mccourt.co	89.145.89.31
2015-05-13	mccourt.co	ns1.ns-mimas.com
2015-05-13	mccourt.co	ns2.ns-mimas.com

Trace forward from the oldest records to the current. See evidence of suspensions, likely change of hands and changes of NS, MX, registrars.


Some malicious actors keep the registrant info when acquiring aged domains, to try to keep the reputation of the domain and attribution pointing to hapless original owner.

- mailprotonmail[.]com
- protonmail[.]systems













Zetalytics DNS History		
Search Term: 217.182.13.249		
Last Seen Q	Domain Q	IP Q
2019-07-24	mailprotonmail.ch	217.182.13.249
2019-07-24	protonmail.systems	217.182.13.249
2019-07-24	mailprotonmail.com	217.182.13.249
2019-06-15	ip249.ip-217-182-13.eu	217.182.13.249
2019-05-28	knpgte250.teknolazer.com.br	217.182.13.249
2019-03-31	bidu250.conveniomedico.emp.br	217.182.13.249
2019-03-06	bidu250.clubedeleads.com.br	217.182.13.249
2019-02-17	bidu250.phdnort.com.br	217.182.13.249
2018-11-14	biju250.grinchdoll.com.br	217.182.13.249
2018-09-28	brnkstr-250.produtosdeorigem.co...	217.182.13.249
2018-02-03	brnkstr-250.tudosjuntos.com.br	217.182.13.249
2017-07-14	pneg250.pensandonegocios.com.br	217.182.13.249
2017-06-01	brnkstr-250.bronkstour.com.br	217.182.13.249
Show Less		


Reverse DNS Host		
Search Term: 217.182.13.249		
Host Q	IP Q	Last Seen Q
ip249.ip-217-182-13.eu	217.182.13.249	2019-07-24
knpgte250.teknolazer.com.br	217.182.13.249	2019-06-12
ppdrdn250.unimedpaulistana.emp...	217.182.13.249	2019-04-10
bidu250.conveniomedico.emp.br	217.182.13.249	2019-03-28
bidu250.clubedeleads.com.br	217.182.13.249	2019-03-21
bidu250.phdnort.com.br	217.182.13.249	2019-02-27
biju250.grinchdoll.com.br	217.182.13.249	2019-01-16
brnkstr-250.produtosdeorigem.co...	217.182.13.249	2018-10-17
brnkstr-250.tudosjuntos.com.br	217.182.13.249	2018-01-31
pneg250.pensandonegocios.com.br	217.182.13.249	2017-07-12
brnkstr-250.bronkstour.com.br	217.182.13.249	2017-05-31


ZONECRUNCHER MX RECORD PIVOT BEARS FRUIT AGAIN




Zetalytics DNS History - Hostnames
Search Term: mailprotonmail.ch
source of data: Zetalytics DNS History

First Seen 	Domain 	Value 
2019-07-24	mailprotonmail.ch	217.182.13.249 
2019-07-23	mailprotonmail.ch	1-you.njalla.no 
2019-07-23	mailprotonmail.ch	you @ can-get-no.info
2019-07-23	mailprotonmail.ch	_acme-challenge.mailprotonmail.ch 
2019-07-23	mailprotonmail.ch	_acme-challenge.www.mailprotonmail.ch 
2019-07-23	mailprotonmail.ch	+4OKrH2Zl9afDw9oE9Ta83zH2Ncgp7sMSU_h4kDZ8_Cs 
2019-07-23	mailprotonmail.ch	+WwsrHU7Ey4-mocUgcgLgO-9E_j0QN8zpmOmtTVyq8Yg 
2019-07-23	mailprotonmail.ch	3-get.njalla.fo 
2019-07-23	mailprotonmail.ch	2-can.njalla.in 
2019-07-22	mailprotonmail.ch	mailprotonmail.ch 

 Show Less



MX to Domain
Search Term: mailprotonmail.ch

qName
withanh.com 

Surprised and delighted to see the patterned behavior tell-tale TTP with the ZoneCruncher pivot of “for the domain we are looking at, has any other domain used it in an MX record?”

Quite rare!

SPECULATION: Test domain for the Man in the MX setup. It makes sense - if I were going to do a sophisticated MitMX that of course I would need to run testing to get it working.











“Sarah with an H” possibly the blog of an innocent person who let their domain expire. The attacker group registers the domain but leaves Sarah’s blog in place as cover.

SIMILARLY FASCINATING MX RECORDS CHRONOLOGY, SAME TTP

After signs that the domain may have changed hands (registrar / NS / host changes) and a long aging pause... Attacker points MX record for withanh[.]com to the SPOOF domain involved in the recent targeted attack: mailprotonmail[.]ch

THEN points withanh[.]com MX record to the REAL ProtonMail service REAL mail[,.]protonmail[.]ch MX hosts, and gets verified with ProtonMail via TXT records.

SPECULATION: setup and testing of MitMX (Man in the Mail eXchanger)

2018-03-27	withanh.com	@protonmail-verification=e3597a528b25e6ea15b14a70618b5bf472ddc4da 
2018-03-03	withanh.com	mail.protonmail.ch 
2018-03-02	withanh.com)v=spf1include:_spf.protonmail.ch mx ~all 
2018-03-02	withanh.com	mailprotonmail.ch 
2017-08-17	withanh.com	69.64.147.10 
2017-08-17	www.withanh.com	69.64.147.10 
2017-08-16	withanh.com	198.54.117.212 
2017-04-10	withanh.com	dns1.registrar-servers.com 
2017-04-10	withanh.com	hostmaster @ registrar-servers.com
2016-09-25	withanh.com	dns2.registrar-servers.com 
2016-09-25	withanh.com	alt1.aspmx.l.google.com 

193.33.61[.]199

- ThreatConnect pivots on an older IP that **mailprotonmail[.]com** pointed to, finding these additional domains with Proton phish potential:
- protonmail[.]direct
- my.secure-protonmail[.]com
- prtn[.]xyz
- Using DNSDB, that's all TC found on the IP. However TC later used a more labor intensive time-fencing technique with other sources to find the rest on this IP.

Zetalytics passive DNS shows more ProtonMail spoof domains on the IP:

The image displays three screenshots from the Zetalytics interface, all filtered by the search term 193.33.61.199.

Netblock Whois Datapoints

Search Term: 193.33.61.199

Country: NL

RIR: RIPE

Creation Date: 2018-01-24

Owner Name: Snel.com B.V.

Email: report@abuse.bz

Status: reassignment

ASN: AS62370 (rank)

PTR NS: ns1.snel.com

Zetalytics DNS History

Search Term: 193.33.61.199

Last Seen	Domain	IP
2019-05-23	actions.protonmail.team	193.33.61.199
2019-06-21	settings.protonmail.systems	193.33.61.199
2019-06-21	user.protonmail.support	193.33.61.199
2019-06-30	mailprotonmail.com	193.33.61.199
2019-07-01	protonmail.systems	193.33.61.199
2019-07-24	protonmail.direct	193.33.61.199
2019-07-24	prtn.xyz	193.33.61.199
2019-07-29	my.secure-protonmail.com	193.33.61.199

Reverse DNS Host

Search Term: 193.33.61.199

Host	IP	Last Seen
server.myserver.com	193.33.61.199	2019-07-10
ho.cockroachaunt.com	193.33.61.199	2019-03-20
hosted-by.snel.com	193.33.61.199	2018-02-14

ZONECRUNCHER HAS MANY BUILT IN PIVOTS

It was easy to find likely related Proton and Prtn spoof domains using pivots like these.

Zetalytics DNS History		
Search Term: 107.170.202.169		
First Seen	Domain	IP
Domain: 'proto' ✕		
2019-04-24	protonmail.earth	107.170.202.169
2019-04-13	secure-protonmail.com	107.170.202.169
Show Less		

Zetalytics DNS History		
Search Term: 107.170.202.169		
First Seen	Domain	IP
Domain: 'prtn' ✕		
2019-04-24	www.prtn.xyz	107.170.202.169
2019-04-11	prtn.xyz	107.170.202.169
Show Less		

Zetalytics DNS History - Hostnames		
Search Term: mailprotonmail.co		
source of data: Zetalytics DNS History		
Last Seen	Domain	Value
2019-07-29	mailprotonmail.co	3-get.njalla.fo
2019-07-29	mailprotonmail.co	2-can.njalla.in
2019-07-24	mailprotonmail.co	1-you.njalla.no
2019-07-24	mailprotonmail.co	you @ can-get-no.info
2019-07-29	mailprotonmail.co	mailprotonmail.co

The Zetalytics API is another way to query through larger result sets than would fit in a browser. Vouch and/or vetting required.

First Seen	Last Seen	Domain	QName	QType	Type	Va
2019-06-27	2019-07-29	prtn.app	prtn.app	6	soa_email	you@can-get-no.info
2019-03-21	2019-07-29	prtn.me	prtn.me	6	soa_email	dns@cloudflare.com
2019-03-12	2019-07-29	prtn.email	prtn.email	6	soa_email	you@can-get-no.info
2018-07-08	2019-07-29	prtn.be	prtn.be	6	soa_email	root@ns01.domainssaubillig.de
2016-09-17	2019-07-29	prtn.com	prtn.com	6	soa_email	hostmaster@1and1.com
2019-06-27	2019-07-29	prtn.app	prtn.app	6	soa_server	1-you.njalla.no
2019-03-21	2019-07-29	prtn.me	prtn.me	6	soa_server	andy.ns.cloudflare.com
2018-07-08	2019-07-29	prtn.be	prtn.be	6	soa_server	ns01.domainssaubillig.de

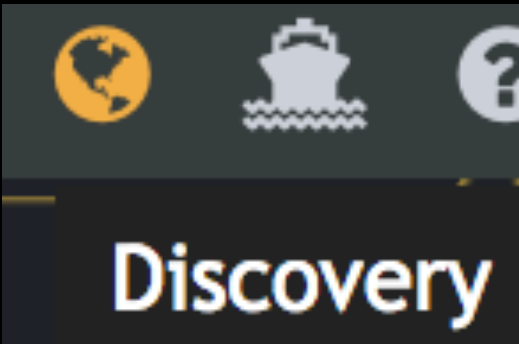
2019-03-17	2019-07-27	prtn.email	prtn.email	15	mx	mail.protonmail.ch
2019-03-17	2019-07-27	prtn.email	prtn.email	15	mx	mailsec.protonmail.ch

ENDLESS SUPPLY SPOOFS

We could keep going with additional finds and likely relate some of them to the current narrow-focus attacker infrastructure.

For now we invite you to join in the effort. Learn from the excellent “Caveats” list at the end of ThreatConnect’s blog post.

Click on the “Discovery” tab in Zetalytics ZoneCruncher for this view:



Power user subscribers can wildcard.

protonmail*

Display Onscreen

Search

Search Period

All

Search Type

Hostname

☒ Last Seen Date

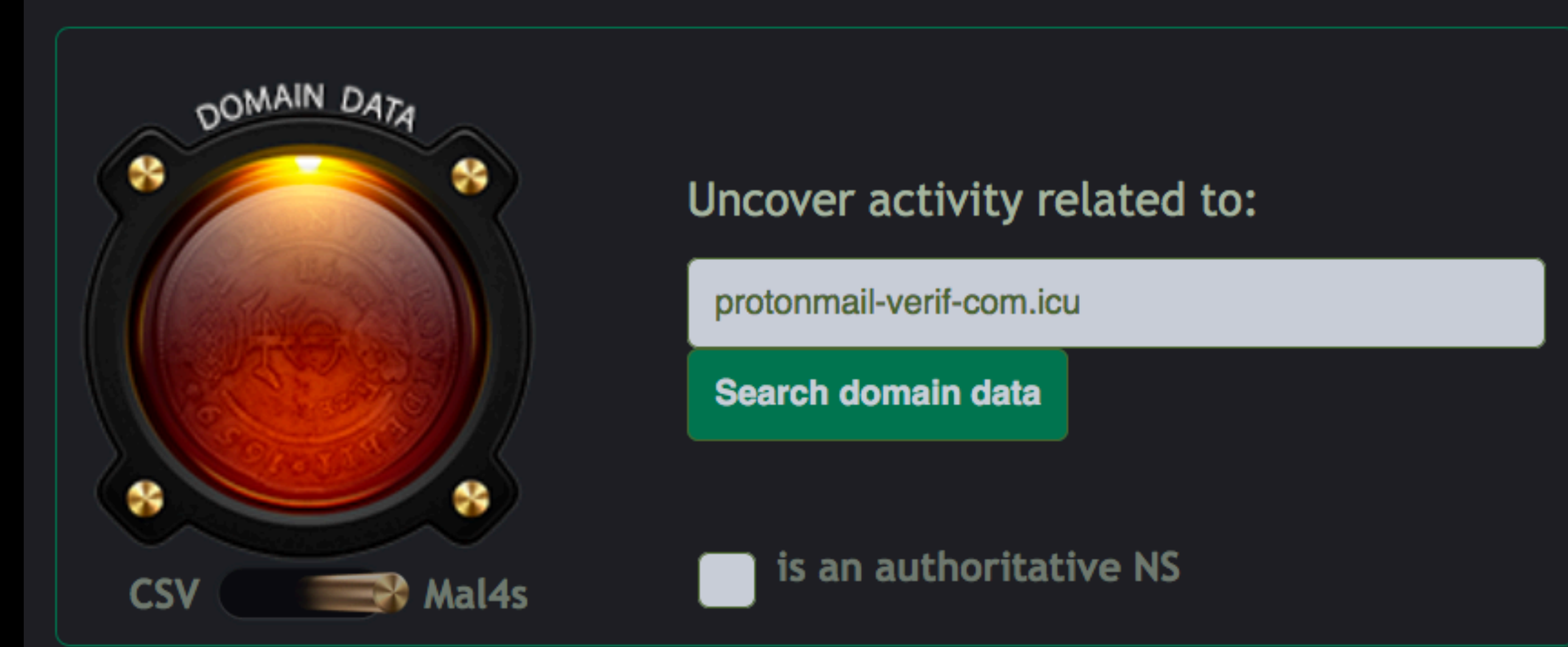
☐ First Seen Date

500 Results Found

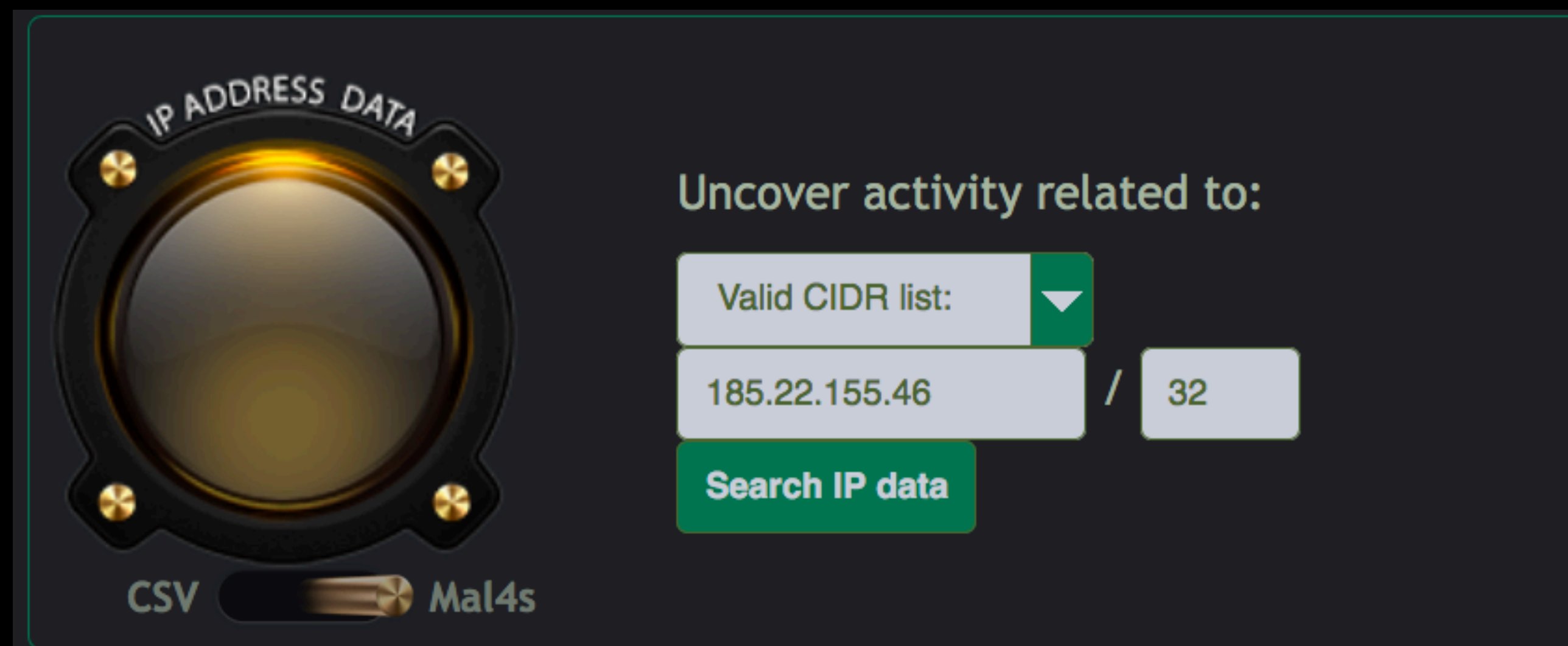
First Seen	Last Seen	Domain	QName	QType	Type	Value
2019-07-29	2019-07-29	protonmail.website	protonmail.website	6	soa_email	admin@expired.reg.ru
2019-07-10	2019-07-29	protonmail-verif-com.icu	protonmail-verif-com.icu	6	soa_email	hostmaster@protonmail-verif-com.icu
2019-06-21	2019-07-29	protonmail.gmbh	protonmail.gmbh	6	soa_email	you@can-get-no.info
2019-06-03	2019-07-29	protonmail.jp	protonmail.jp	6	soa_email	hostmaster@iwantmyname.com
2019-05-30	2019-07-29	protonmail-security.com	protonmail-security.com	6	soa_email	hostmaster@gandi.net
2019-05-06	2019-07-29	protonmail.team	protonmail.team	6	soa_email	you@can-get-no.info
2019-04-25	2019-07-29	protonmail.earth	protonmail.earth	6	soa_email	info@web4africa.net
2019-04-09	2019-07-29	protonmail.cc	protonmail.cc	6	soa_email	hostmaster@transip.nl
2019-03-08	2019-07-29	protonmaillist.ru	protonmaillist.ru	6	soa_email	noc@parkline.ru
2019-03-06	2019-07-29	protonmail.vip	protonmail.vip	6	soa_email	you@can-get-no.info
2019-07-29	2019-07-29	protonmail.website	protonmail.website	6	soa_server	ns1.expired.reg.ru
2019-07-10	2019-07-29	protonmail-verif-com.icu	protonmail-verif-com.icu	6	soa_server	ns1.justhost.ru
2019-06-21	2019-07-29	protonmail.gmbh	protonmail.gmbh	6	soa_server	1-you.njalla.no
2019-06-03	2019-07-29	protonmail.jp	protonmail.jp	6	soa_server	ns1.iwantmyname.net
2019-05-30	2019-07-29	protonmail-security.com	protonmail-security.com	6	soa_server	ns1.gandi.net
2019-05-06	2019-07-29	protonmail.team	protonmail.team	6	soa_server	1-you.njalla.no
2019-04-25	2019-07-29	protonmail.earth	protonmail.earth	6	soa_server	ns1.web4africa.com
2019-04-09	2019-07-29	protonmail.cc	protonmail.cc	6	soa_server	ns0.transip.net

NEXT STEPS – FOLLOW UPS

- Get a ZoneCruncher subscription - [click here](#)
- Have questions?
- Schedule a screensharing session: calendly.com/zetalytics
- Keep pivoting - there's much more to discover about the ProtonMail spoofing infrastructure and the many different actors who will make a go of it.



ZETalytics



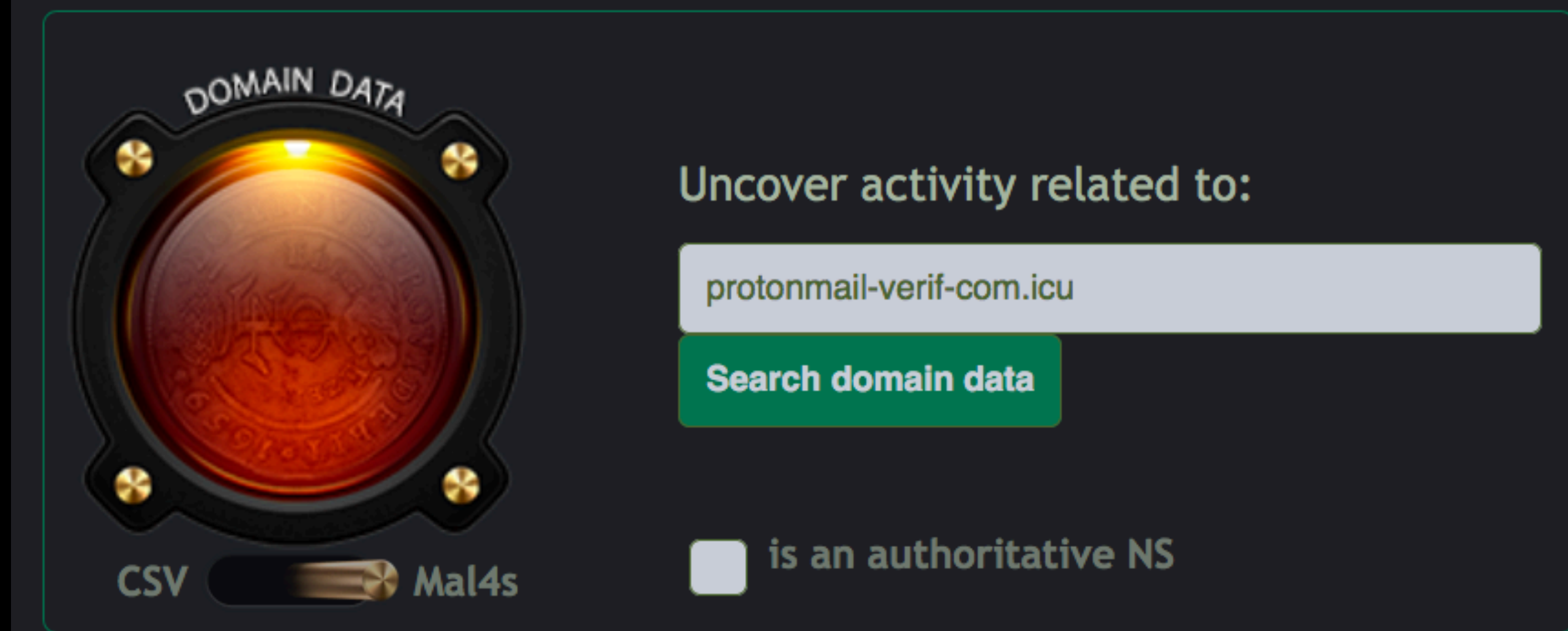
HIGH RISK THREAT INTEL FEEDS

Zetalytics customers were protected from protonmail[.]sh on June 27th 2019 starting at 17:52:36 UTC.

We use statistical, behavioral, relationship and resource methods to classify high risk and high confidence malicious domains and CIDRs.

Like many of the ProtonMail spoof domains we listed on June 21st 2019 - malicious use cases may be a mystery but blocking is pre-emptive.

If you're protecting journalists, enterprise networks or critical infrastructure, give our feeds a try.



DOMAIN DATA

Uncover activity related to:

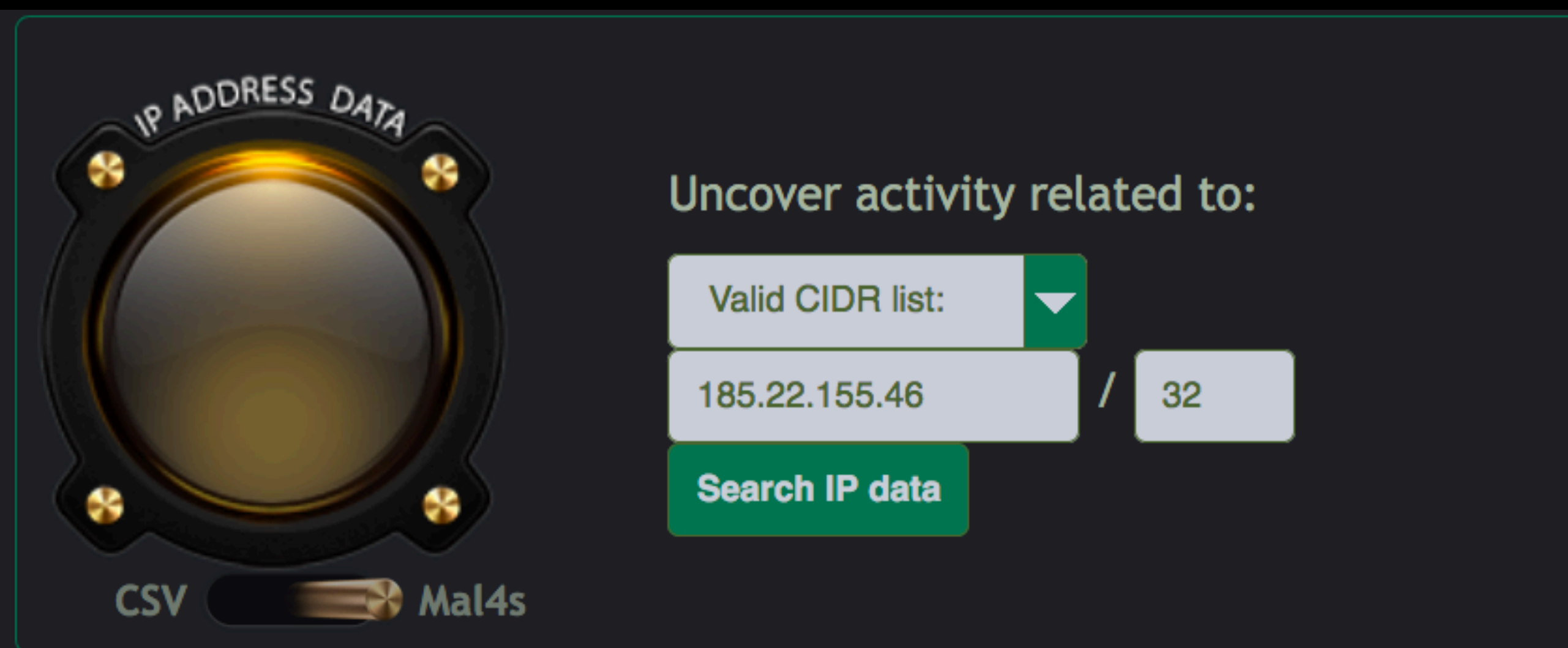
protonmail-verif-com.icu

Search domain data

CSV Mal4s

☐ is an authoritative NS

ZETALytics



IP ADDRESS DATA

Uncover activity related to:

Valid CIDR list: ▼

185.22.155.46 / 32

Search IP data

CSV Mal4s

[Twitter: @zetalytics.com](#)

EXERCISE COMPLETED

**KNOW SOMEONE WHO NEEDS
PASSIVE DNS DATA
TOOLS, TRAINING, THREAT INTEL?**

Send them our way 😎

ZETAlytics

tml@Zetalytics.com