Bite-Size Exercise

c2 pivots with interesting results

APRIL LORENZEN
Chief Data Scientist
Twitter: @zetalytics.com

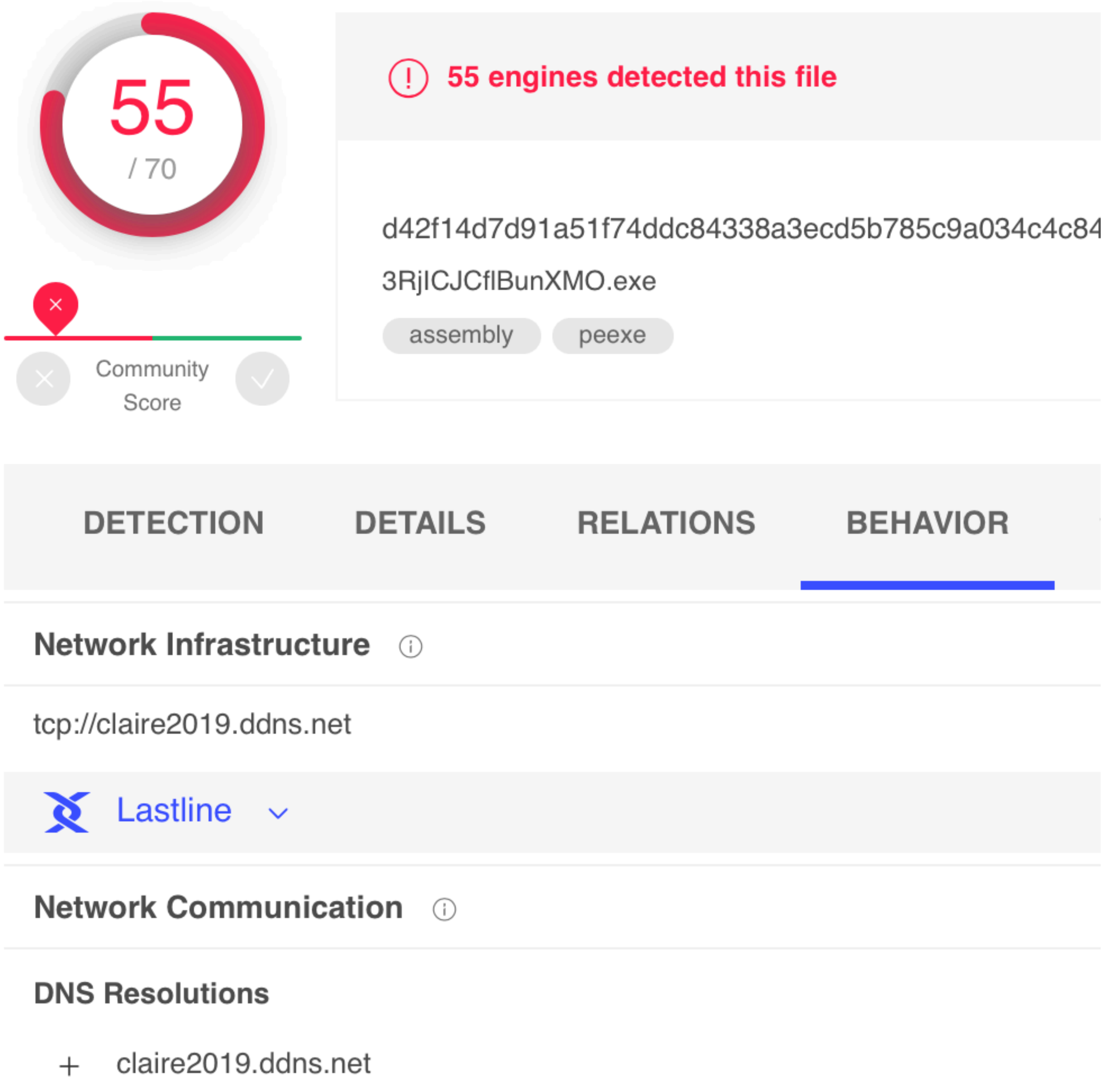
ZETAlytics

AGENDA

- *Pluck c2 from malware network traffic*
- *Use high quality pivots - expand without time-wasting garbage*
- *Find related infra and activity:*
  - *Blocklist the things*
  - *Monitor the things*
  - *Attribution clues*

FIND A C2 FOR OUR TEST

- ➤ Search urlhaus for newest **online** malware download
- ➤ Use tor to download the EXE file
- ➤ Upload to virus total
- ➤ Click on BEHAVIOR tab



55 / 70

55 engines detected this file

d42f14d7d91a51f74ddc84338a3ecd5b785c9a034c4c84

3RjICJCflBunXMO.exe

assembly peexe

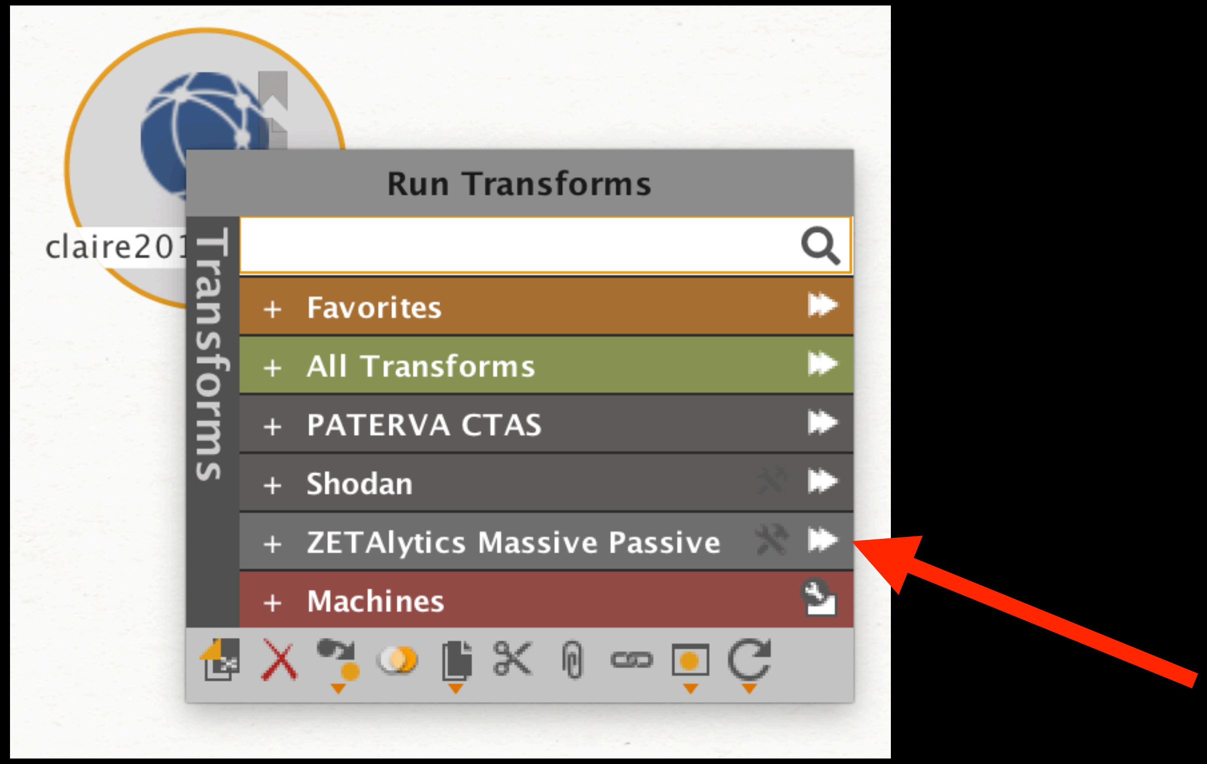
Network Infrastructure

tcp://claire2019.ddns.net

Network Communication

DNS Resolutions

+ claire2019.ddns.net

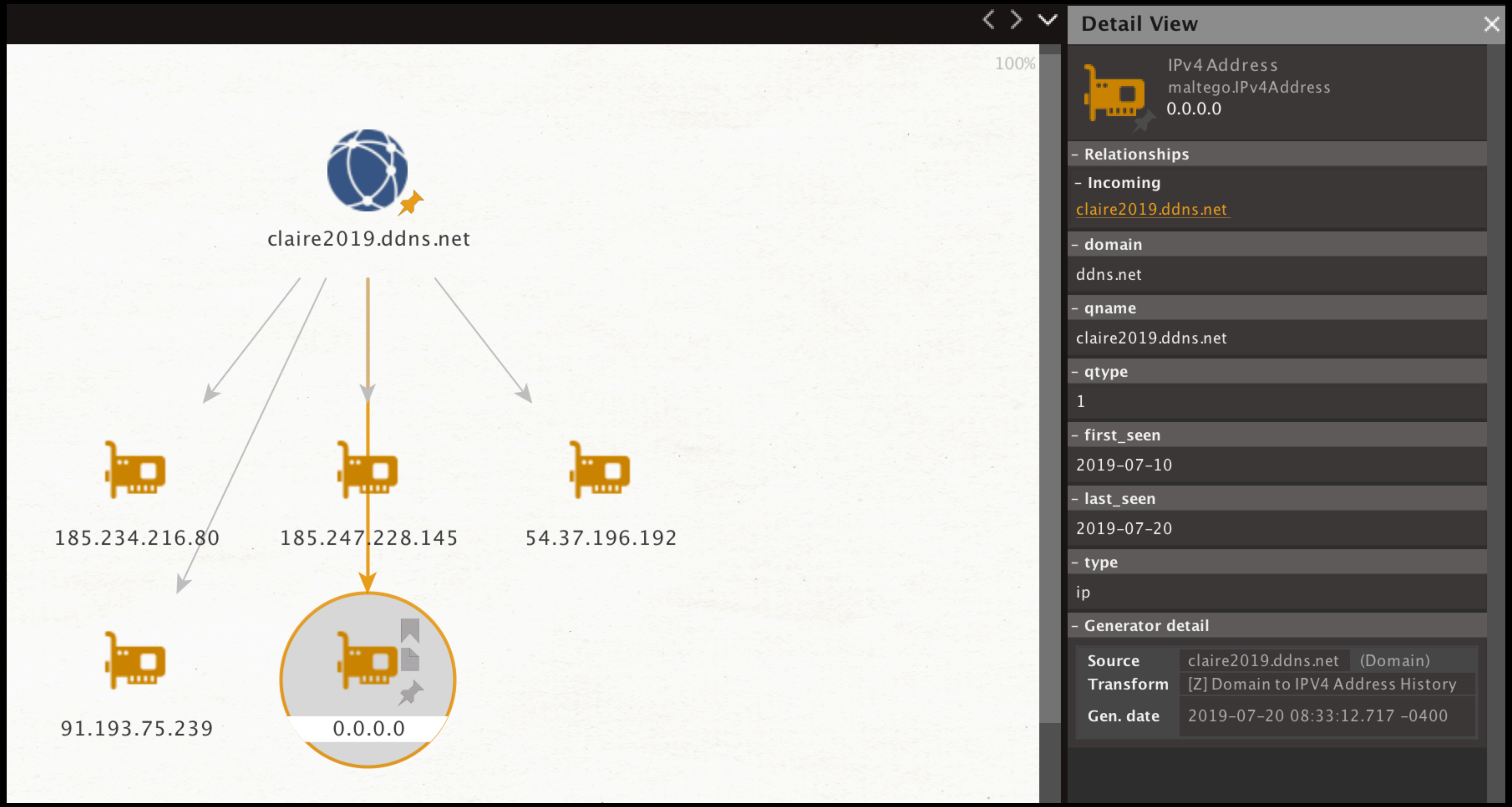


Using Maltego (free instant access to Zetalytics transforms API key)

Drag out a “Domain” or “DNS Name” entity type, paste in claire2019.ddns.net

Click on the ▶ next to ZETAlytics Massive Passive.

▶ runs all applicable ZETAlytics transforms with minimal effort.



Detail View

IPv4 Address
maltego.IPv4Address
0.0.0.0

- Relationships
- Incoming
claire2019.ddns.net

- domain
ddns.net

- qname
claire2019.ddns.net

- qtype
1

- first_seen
2019-07-10

- last_seen
2019-07-20

- type
ip

- Generator detail

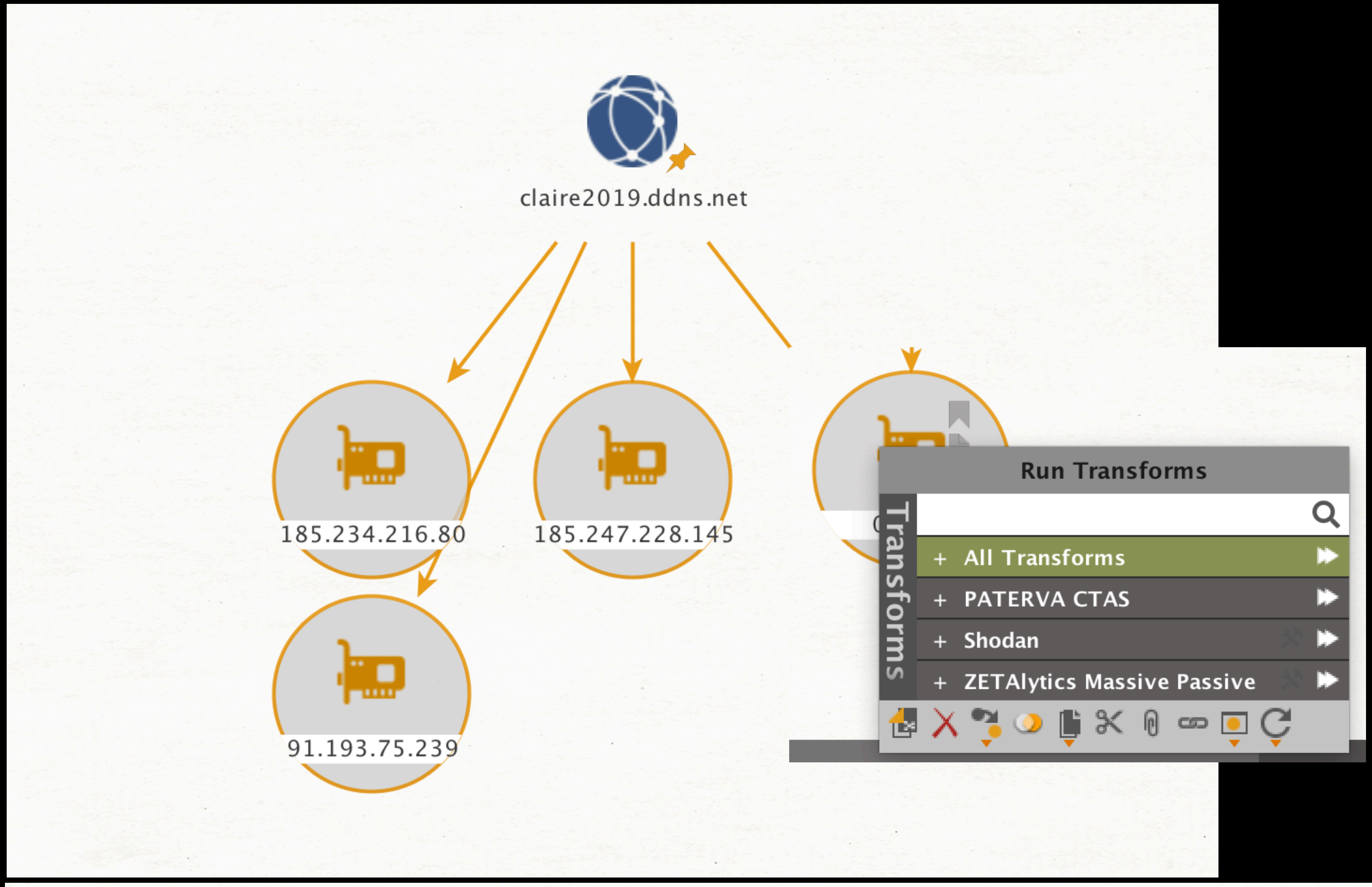
Source	claire2019.ddns.net (Domain)
Transform	[Z] Domain to IPV4 Address History
Gen. date	2019-07-20 08:33:12.717 -0400

ZETAlytics passive DNS has seen this c2 hostname resolving to 5 IPs. Most recently, 0.0.0.0 because the DDNS operator pointed the malicious host there to incapacitate it.

Our goal is to find strongly correlated infrastructure of the same actor, while avoiding garbage results.

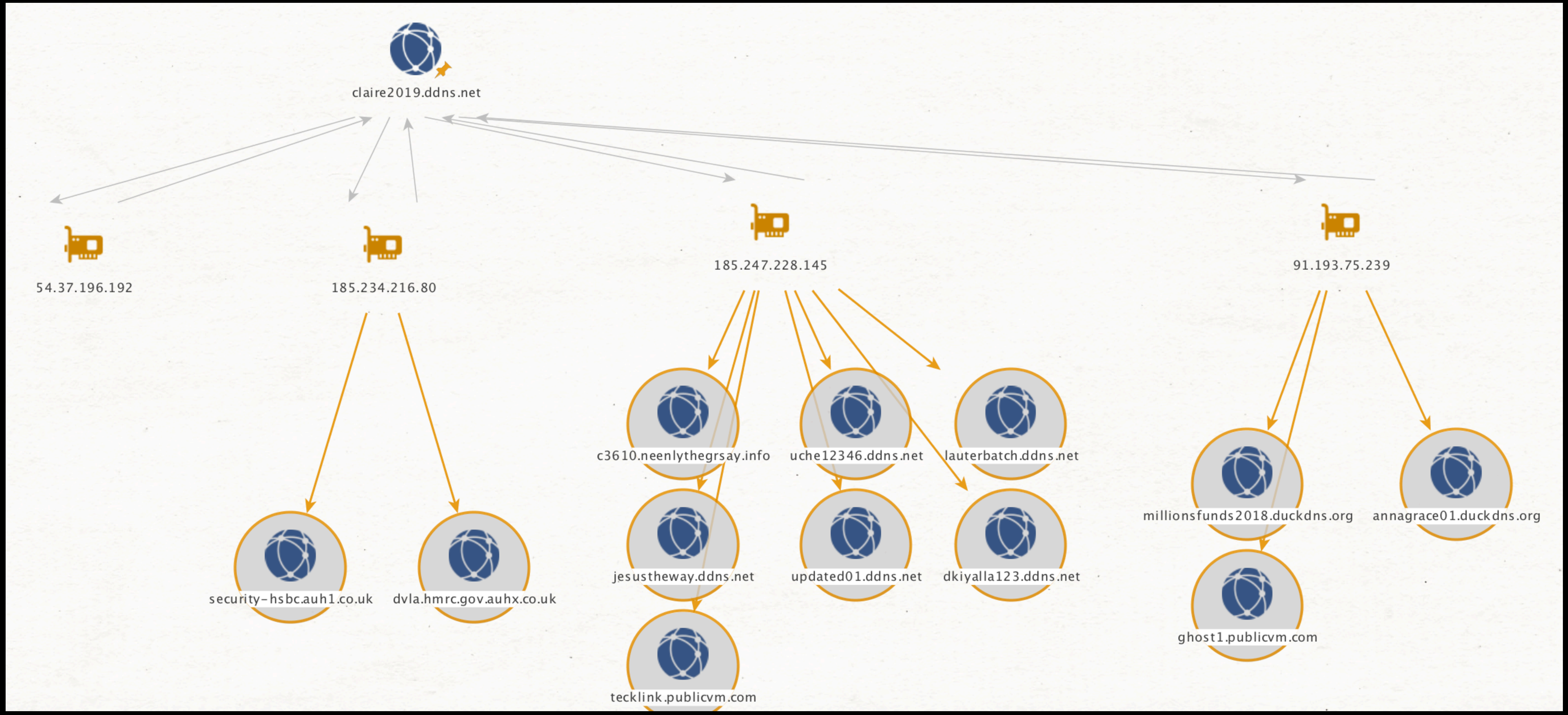
➤ Highlight and **delete the 0.0.0.0 IP** to avoid expanding to irrelvant unrelated infrastructure.

Same pivot techniques work in our ZoneCruncher web portal or scripted with our JSON API



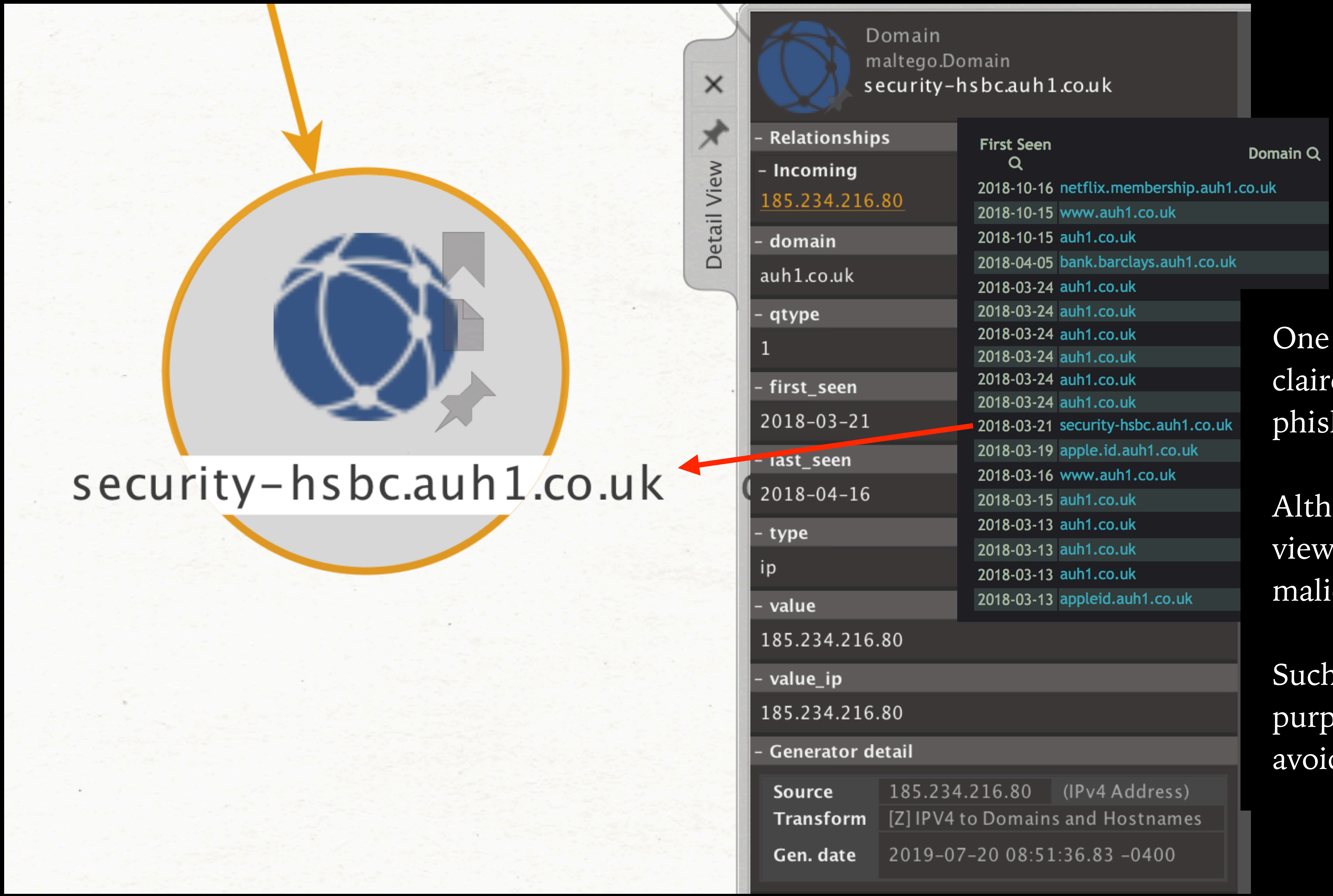
Highlight the 4 IPs

RUN ALL again on the Zetalytics Massive Passive ▶



The results from passive DNS show us hostnames that used these IPs historically

Quite a few interesting dynamic dns hosts have shared the same IPs as claire2019.ddns.net



Domain
maltego.Domain
security-hsbc.auh1.co.uk

- Relationships
- Incoming
185.234.216.80
- domain
auh1.co.uk
- qtype
1
- first_seen
2018-03-21
- last_seen
2018-04-16
- type
ip
- value
185.234.216.80
- value_ip
185.234.216.80
- Generator detail

Source	185.234.216.80 (IPv4 Address)
Transform	[Z] IPV4 to Domains and Hostnames
Gen. date	2019-07-20 08:51:36.83 -0400

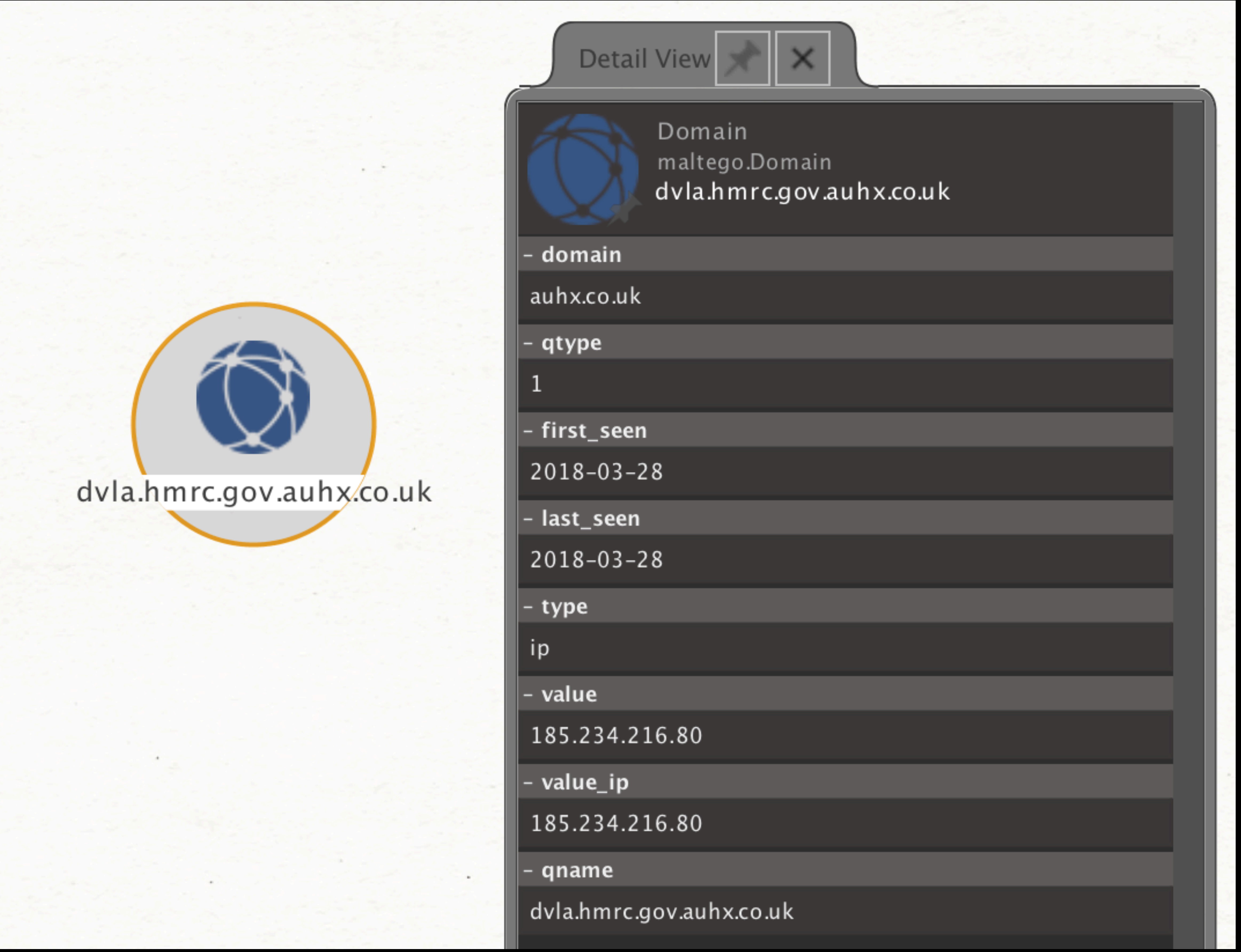
First Seen	Domain
2018-10-16	netflix.membership.auh1.co.uk
2018-10-15	www.auh1.co.uk
2018-10-15	auh1.co.uk
2018-04-05	bank.barclays.auh1.co.uk
2018-03-24	auh1.co.uk
2018-03-24	auh1.co.uk
2018-03-24	auh1.co.uk
2018-03-24	auh1.co.uk
2018-03-24	auh1.co.uk
2018-03-24	auh1.co.uk
2018-03-21	security-hsbc.auh1.co.uk
2018-03-19	apple.id.auh1.co.uk
2018-03-16	www.auh1.co.uk
2018-03-15	auh1.co.uk
2018-03-13	auh1.co.uk
2018-03-13	auh1.co.uk
2018-03-13	auh1.co.uk
2018-03-13	appleid.auh1.co.uk

One of the hosts sharing an IP with the c2 claire2019.ddns.net has been used for multiple phishing child labels in 2018.

Although no longer active, having the historical view helps in assessing the probability of current malicious activity.

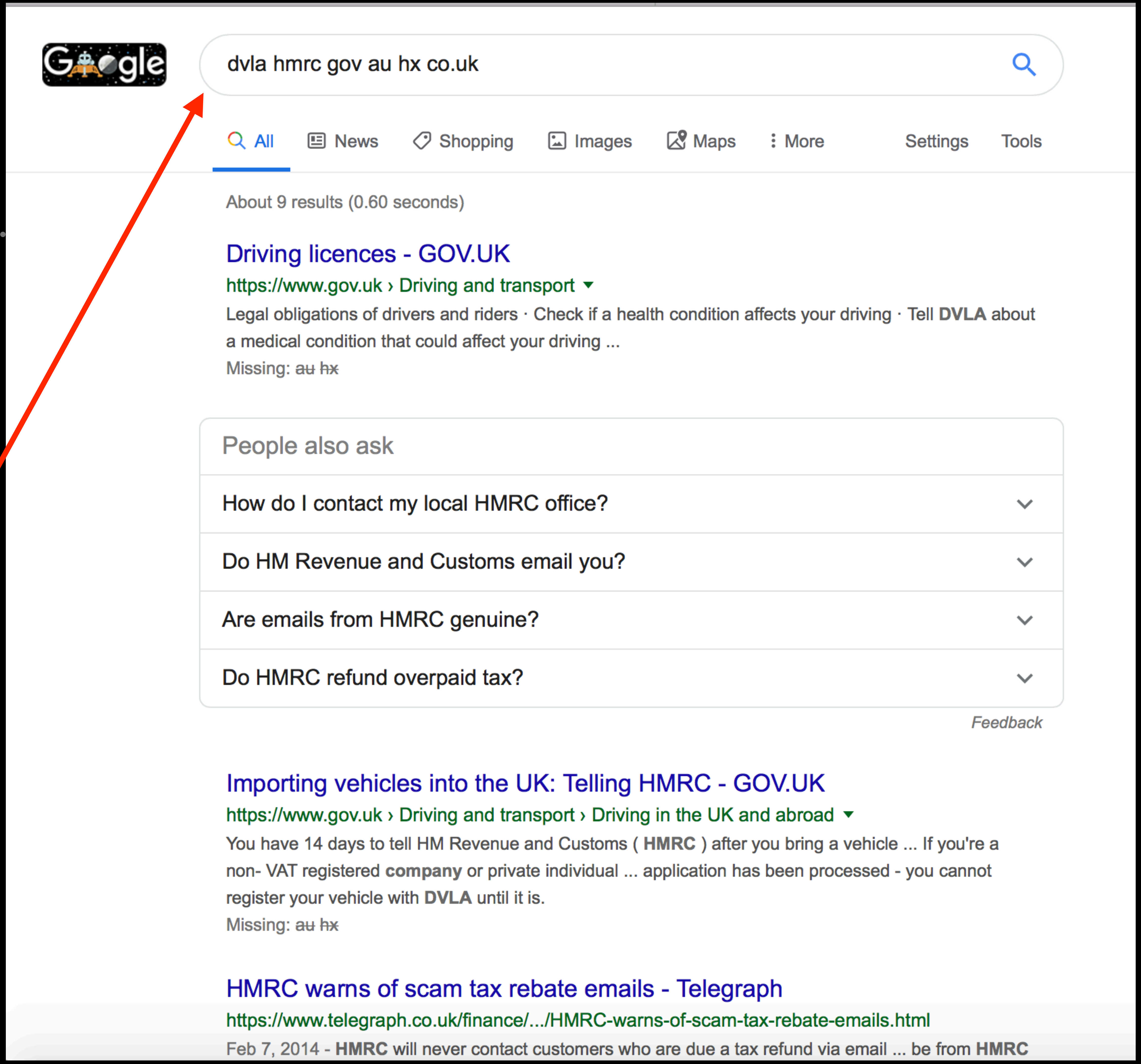
Such data can be used in AI / ML models, and serve purposes such as false positive and false negative avoidance.

Another host sharing an IP with the c2 claire2019.ddns.net has been used for a phish of a United Kingdom Driving License official site. Note the similar, but not same, base domain of auhx.co.uk vs auh1.co.uk



Domain
maltego.Domain
dvla.hmrc.gov.auhx.co.uk

- domain
auhx.co.uk
- qtype
1
- first_seen
2018-03-28
- last_seen
2018-03-28
- type
ip
- value
185.234.216.80
- value_ip
185.234.216.80
- qname
dvla.hmrc.gov.auhx.co.uk



dvla hmrc gov au hx co.uk

About 9 results (0.60 seconds)

Driving licences - GOV.UK
https://www.gov.uk › Driving and transport
Legal obligations of drivers and riders · Check if a health condition affects your driving · Tell **DVLA** about a medical condition that could affect your driving ...
Missing: ~~au~~ ~~hx~~

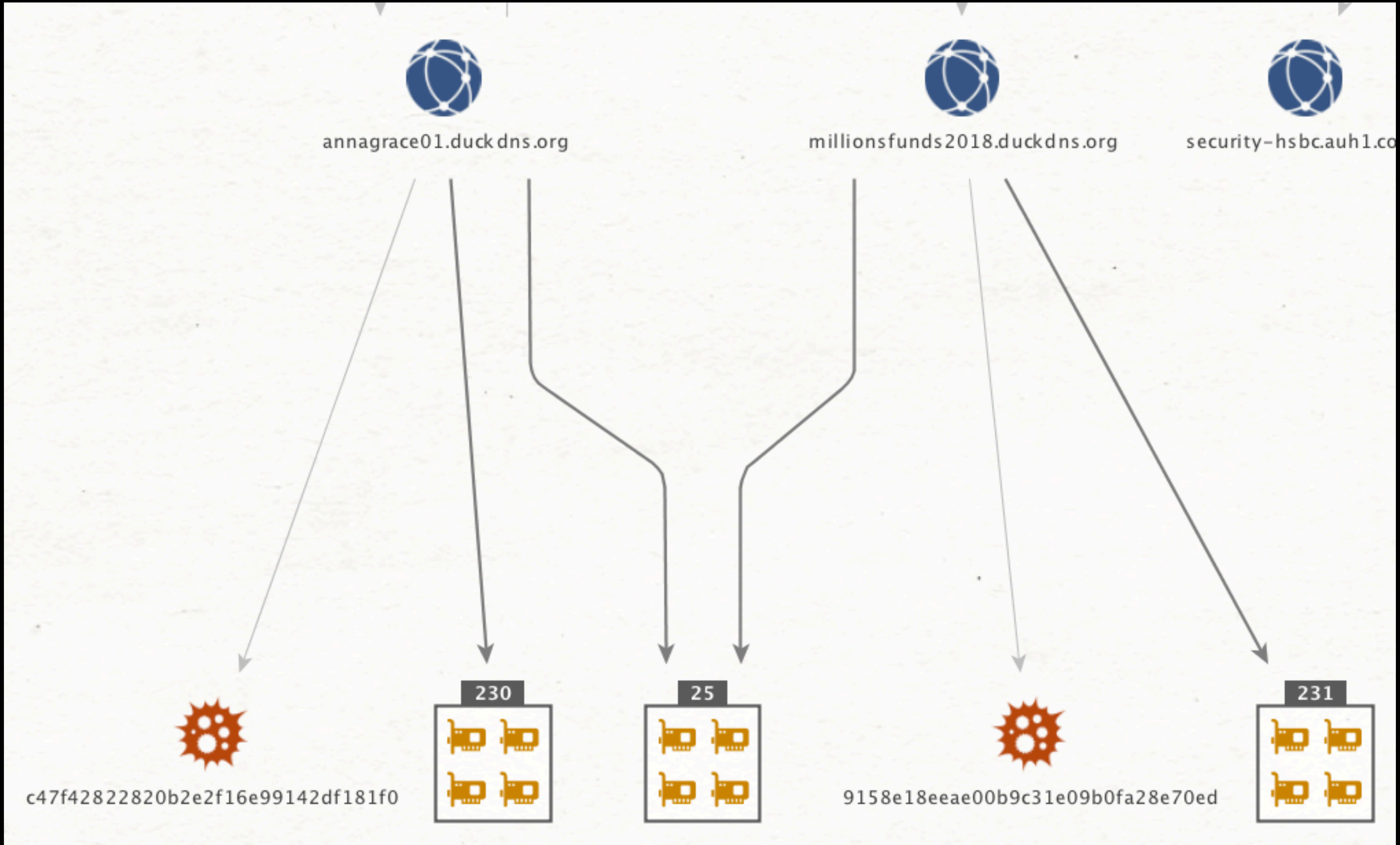
People also ask
How do I contact my local HMRC office?
Do HM Revenue and Customs email you?
Are emails from HMRC genuine?
Do HMRC refund overpaid tax?
Feedback

Importing vehicles into the UK: Telling HMRC - GOV.UK
https://www.gov.uk › Driving and transport › Driving in the UK and abroad
You have 14 days to tell HM Revenue and Customs (**HMRC**) after you bring a vehicle ... If you're a non- VAT registered **company** or private individual ... application has been processed - you cannot register your vehicle with **DVLA** until it is.
Missing: ~~au~~ ~~hx~~

HMRC warns of scam tax rebate emails - Telegraph
https://www.telegraph.co.uk/finance/.../HMRC-warns-of-scam-tax-rebate-emails.html
Feb 7, 2014 - **HMRC** will never contact customers who are due a tax refund via email ... be from **HMRC**

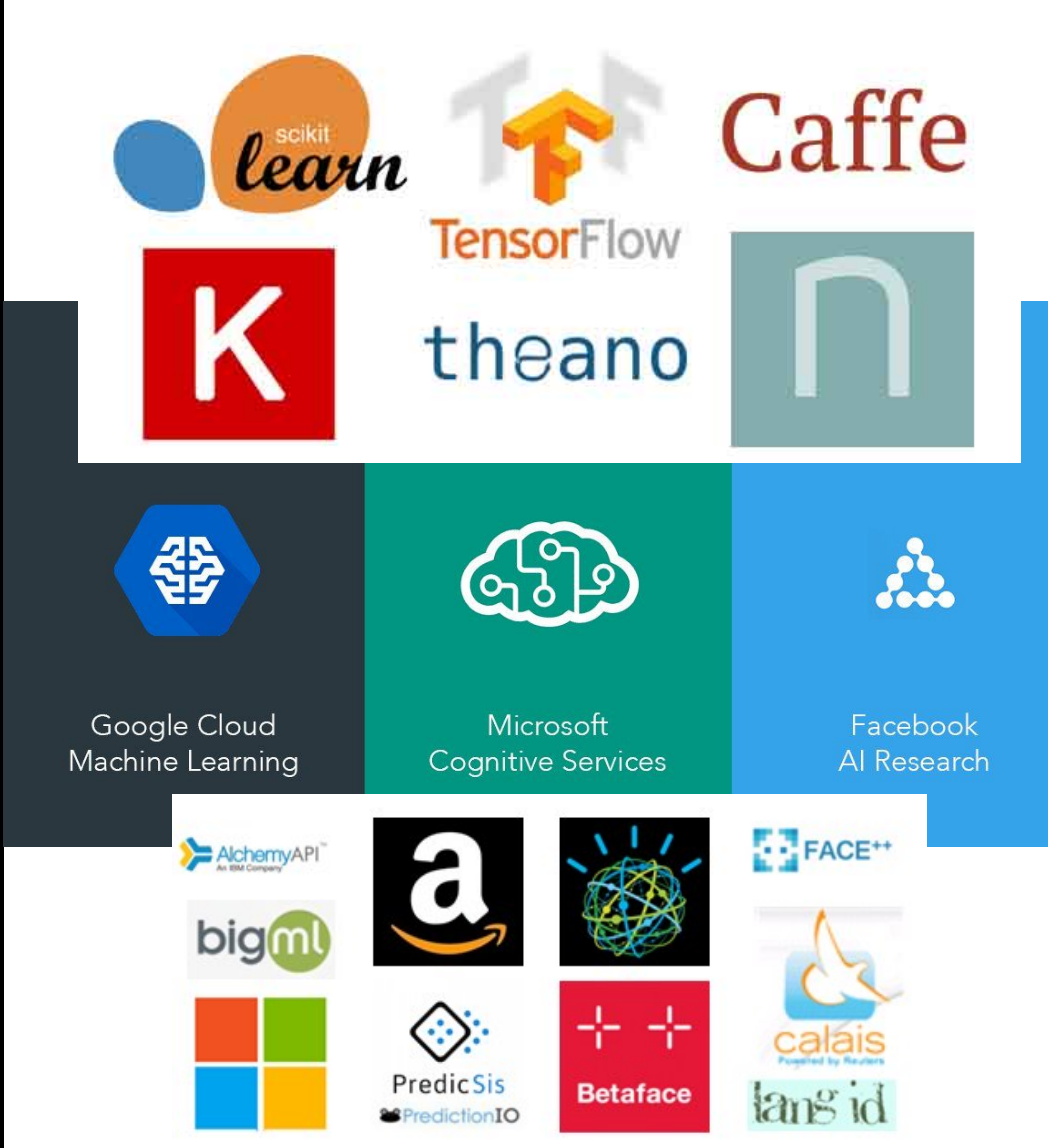
TIP: break the hostname apart with spaces in order to help find relevant “real site” results in a search engine.

Malware is associated with multiple hostnames that have shared the IP space with our starting c2 host, claire2019.ddns.net. Importantly, there's just a small number of hostnames pointing at these IPs - which increases the probability of one actor or group carrying out the activities.


annagrace01.duckdns.org
millionsfunds2018.duckdns.org
security-hsbc.auh1.co
c47f42822820b2e2f16e99142df181f0
230
25
9158e18eeae00b9c31e09b0fa28e70ed
231

NEXT STEPS - FOLLOW UPS

- ➤ Could make great inputs for your AI/ML models
- ➤ Have questions?
- ➤ Schedule a screensharing session: calendly.com/zetalytics
- ➤ Keep pivoting - there's much more to discover about this c2 😎



Twitter: @zetalytics.com

EXERCISE COMPLETED

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

Send them our way 😎

ZETAlytics

tml@Zetalytics.com