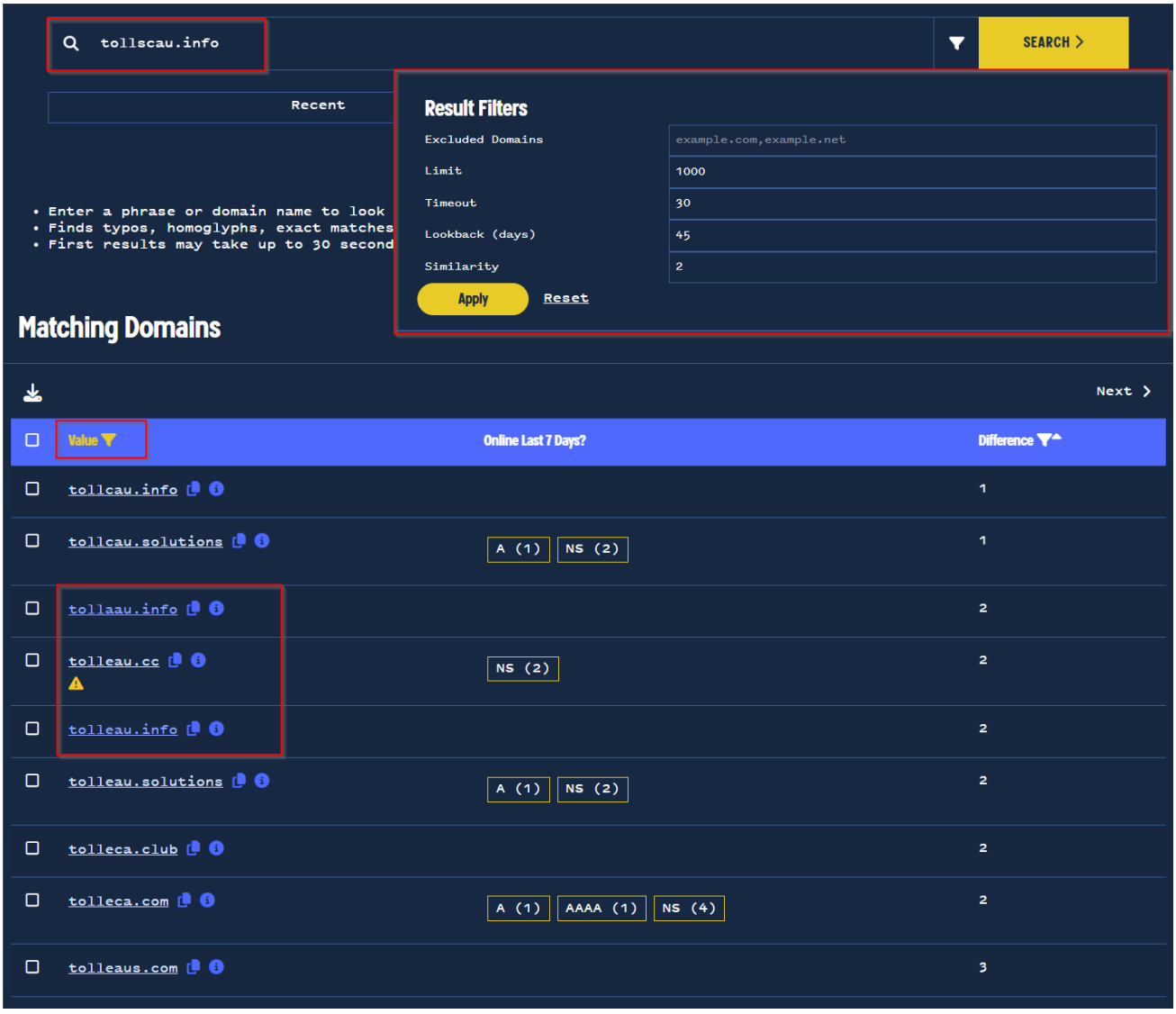
Revealing Spammer Infrastructure With Passive DNS - 226 Toll-Themed Domains Targeting Australia

validin.com/blog/revealing-spammer-infrastructure-with-passive-dns-au-toll-smishing/

May 15, 2024

Portal



By: Matthew @ Embee Research

2024-05-15

general

How to analyze spam domains with passive DNS history

Introduction

We've all seen those annoying spam messages that prompt us to click on links related to outstanding payments. But have you ever wondered how to analyse them?

Today, we'll investigate one such text sent to an Australian researcher. This text leveraged social engineering to trick the victim into clicking the link and paying a bogus outstanding Toll payment.

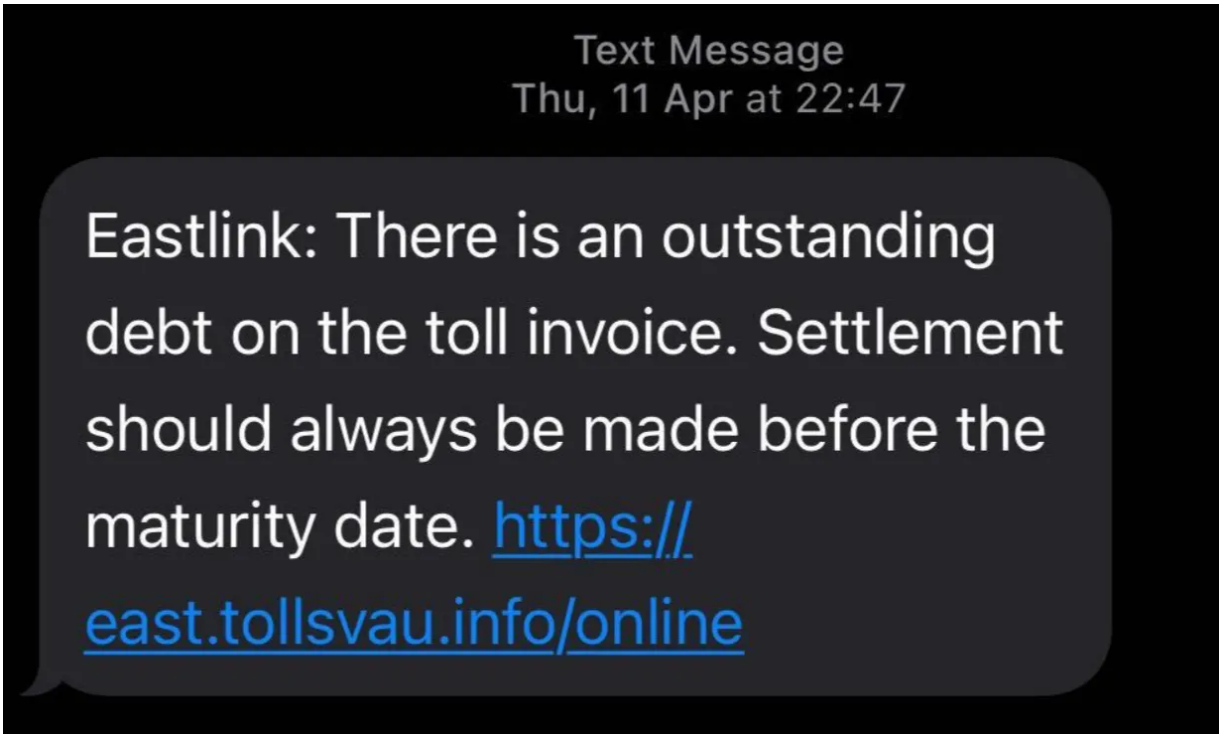
We'll leverage passive DNS analysis to reverse engineer the domain infrastructure of the link within the text, and historical IP records to identify additional domains linking to the same infrastructure.

This combination will ultimately lead to 226 unique domains targeting Australian users with messages impersonating the EastLink toll service.

Obtaining An Initial Indicator

On April 11th, we received a suspicious text message that attempted to social engineer us into clicking on a suspicious link for the domain `east.tollsvau[.]info`.

This message was sent to an Australian researcher and attempted to impersonate the Melbourne-based EastLink toll service



Toll road smishing targeting Australian residents.

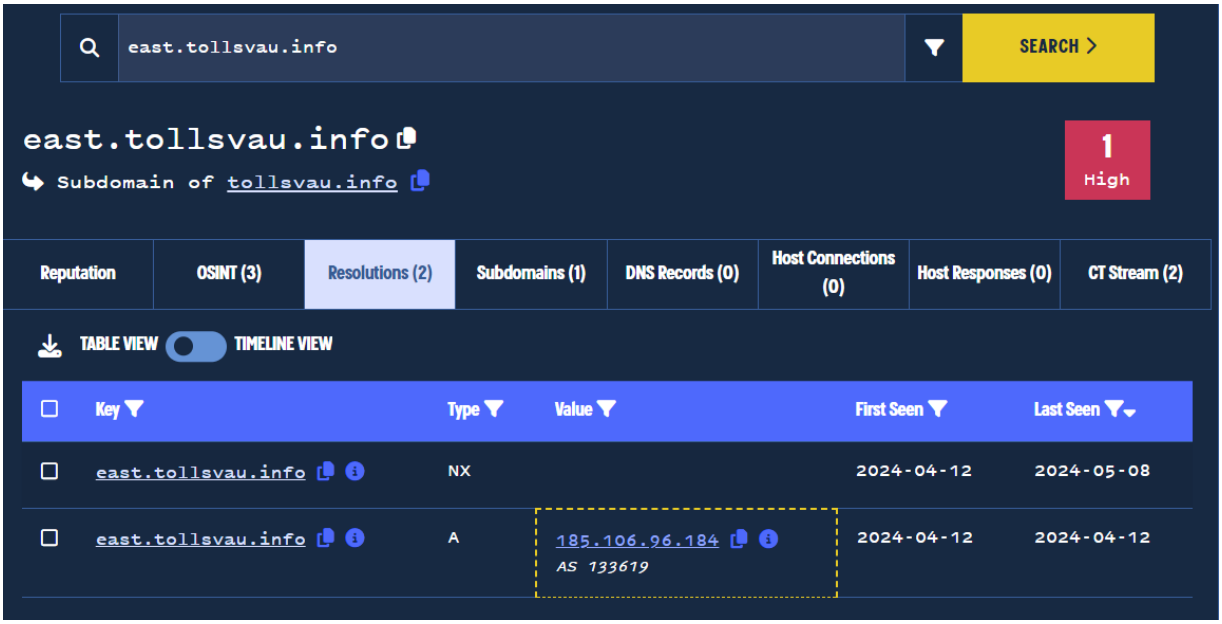
We initially ignored the text as it looked like generic spam that would prompt us to input some credentials or make a bogus payment that would be sent to the spam author.

We later realised that we could have much more fun with this message, and we decided to analyse it and see just how many other similar domains we could find.

Obtaining the IP Address of the Domain

Our first step was to obtain the IP address of the domain by performing a passive DNS lookup on `east.tollsvau[.]info`.

This revealed a single associated IP address of `185.106.96[.]184` which was first seen on `2024-04-12`.



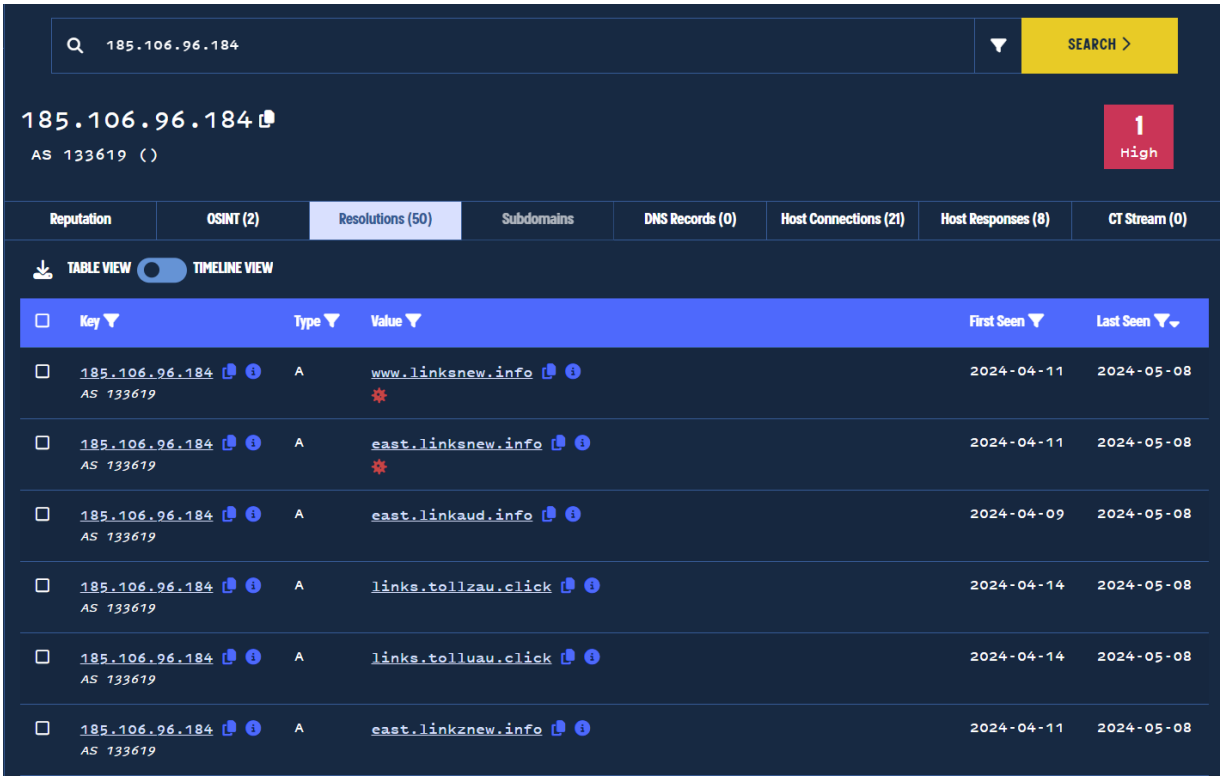
Obtaining IP address history for a domain

Pivoting on The IP Address to Find New Domains

Our next step was to analyse the IP address and observe any other domains that have resolved to the same address.

We did this by clicking on `185.106.96[.]184`, which will automatically perform a reverse passive DNS lookup and display any domains pointing to the same IP.

This simple pivot revealed 50 associated domains, 42 of which were first seen within days of `east.tollsvau[.]info`, and all contained toll-related themes primarily targeting Australia.



Pivoting on PDNS IP history to find new domains.

Scrolling through our results, we can observe that the first toll-themed domain was seen on April 9, 2024.

We observed 42 results with toll themes, and 8 results from 2023 that featured themes unrelated to tolls and spamming. These 8 unrelated domains are likely part of a different campaign or are artifacts of a previous owner of the address. We ignored these older domains as our goal was on the toll campaign.

Finding the earliest relevant date for domains pointing to this IP.

Of the 42 resulting domains (including subdomains), there were 21 unique apex domains with toll-related themes.

Output

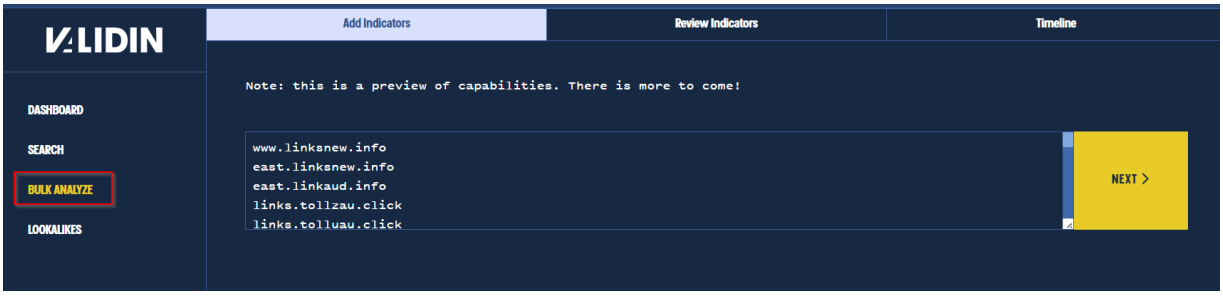
```
eastlinkau.click
eastlinks.click
linkanew.info
linkaud.info
linkauf.info
linkaui.info
linkauj.info
linkaul.info
linkaur.info
linkcnew.info
linksnew.info
linkznew.info
tollnau.click
tollscau.info
tollseau.info
tollsuau.info
tollsvau.info
tolluau.click
tollvau.info
tollzau.click
tollzau.info
```

Unique apex domains with toll phishing themes.

Pivoting To Additional Domains

Similar to our search on the initial domain indicator `east.tollsvau[.]info`, we can resolve the newly identified domains to identify historical IP addresses that could lead to additional infrastructure.

To speed up this process, we used Validin's Bulk Analyze feature to resolve and analyse all domains in a single search.



Using bulk DNS analyze to speed up analysis.

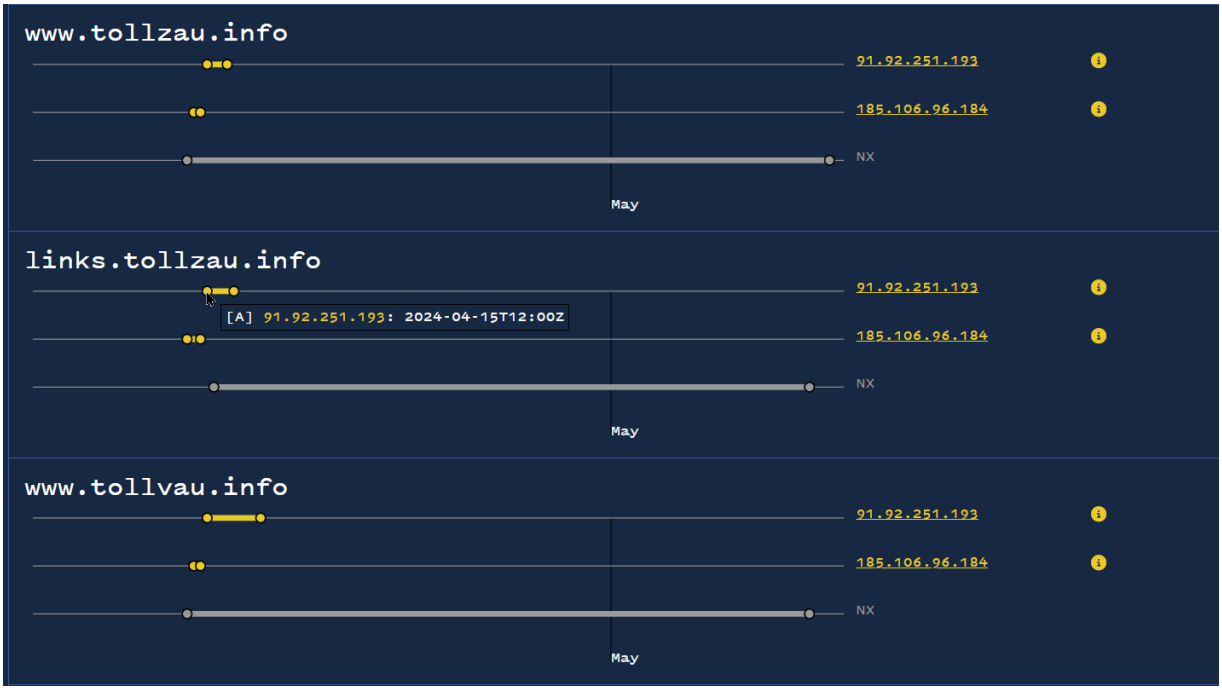
A Bulk Analyze search shows us historical addresses and timelines for each of the provided domains.

This allows us to easily visualise the results and reveals that most domains have only ever resolved to a single IP address, the same `185.106.96[.]184` as our initial indicator.

Visualizing overlap with IP history using bulk DNS analysis.

However, if we scroll through the complete results of the Bulk Analyze search, we can see that some domains switched to `91.92.251[.]193` around April 15, 2024.

Of our initial 42 results, 6 of the domains had made this switch

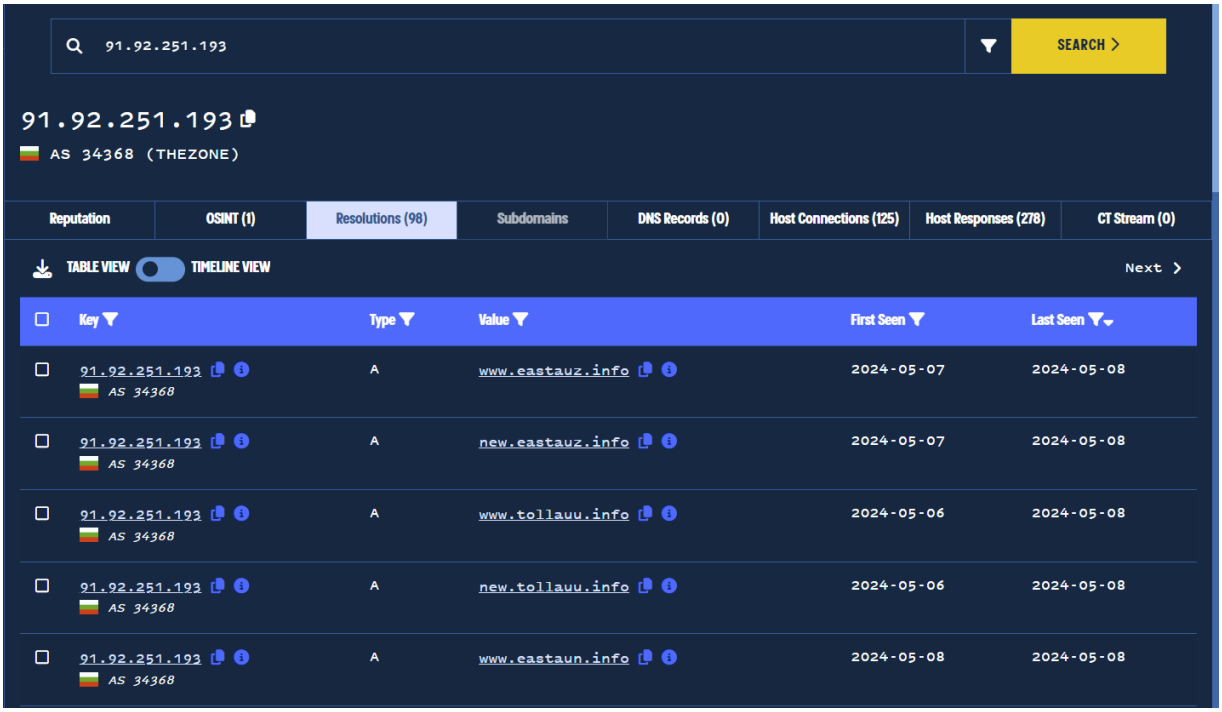


Bulk analysis highlights IP change in PDNS history.

We wanted to find additional domains related to `91.92.251[.]193`, so we performed an additional pivot by clicking on the address.

This automatically performed another lookup, which revealed 98 associated domains.

93 of these domains featured Australian Toll-related themes, beginning from `April 15, 2024`. 5 of the domains were unrelated to tolls and were likely from a previous owner.



IP address pivot reaveals many new Austrailian toll-themed phishing domains.

The first toll-themed domain on `91.92.251[.]193` appeared on `April 15th, 2024`. The domains prior to this date appeared to be unrelated.

First seen date for IP associations distinguishes related domains.

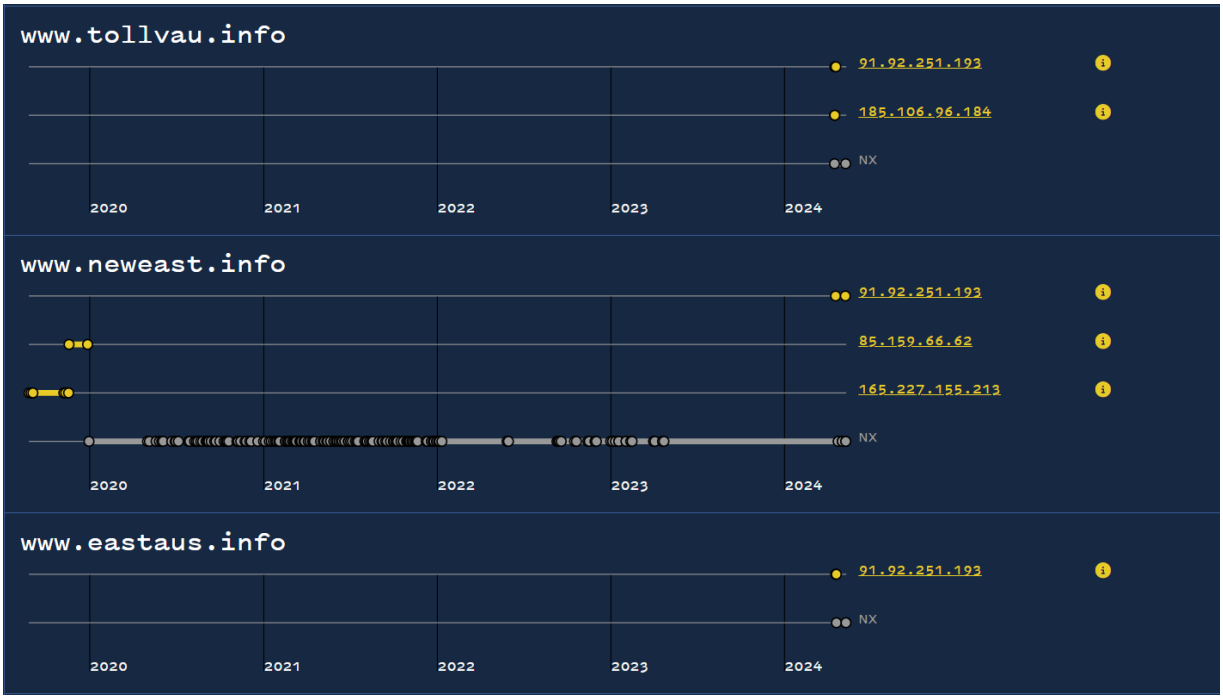
We added these new domains to the results of our initial search. This meant that we now had 128 domains (including subdomains) across 63 unique apex domains.

IP pivot results in 63 unique apex domains.

We performed another bulk analyse lookup on the new domains in an attempt to find any IP addresses that lead to additional infrastructure.

Sadly, all 128 domains featured only `185.106.96[.]184` and `91.92.251[.]193` which we had already analyzed. This meant that we had exhausted our IP-based pivots and would need to use to other options.

The few additional IPs (like `165.227.155[.]213` below) were years old and led only to domains completely unrelated to our Australian toll theme.

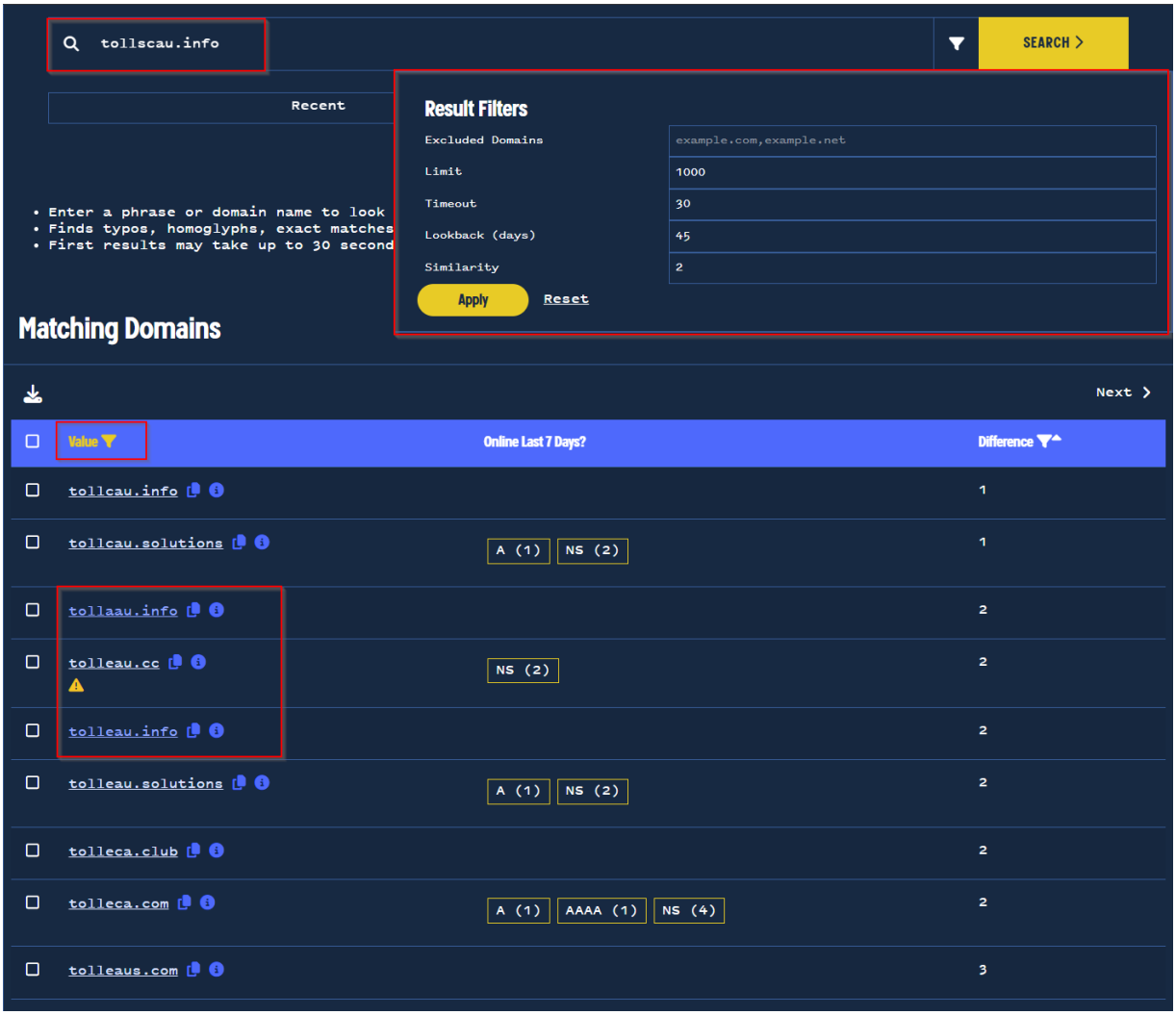


Visualizing domains in bulk helps confirm unrelated pivots.

Locating Additional Indicators With Lookalike Searches

We had exhausted our options for IP-based pivots, so we decided to try a lookalike search to identify domains with names that closely matched those that we had identified.

By running a lookalike search on one such domain `tollscau[.]info` and applying a string filter of `toll`, we were able to identify new domains with extremely similar naming schemes.



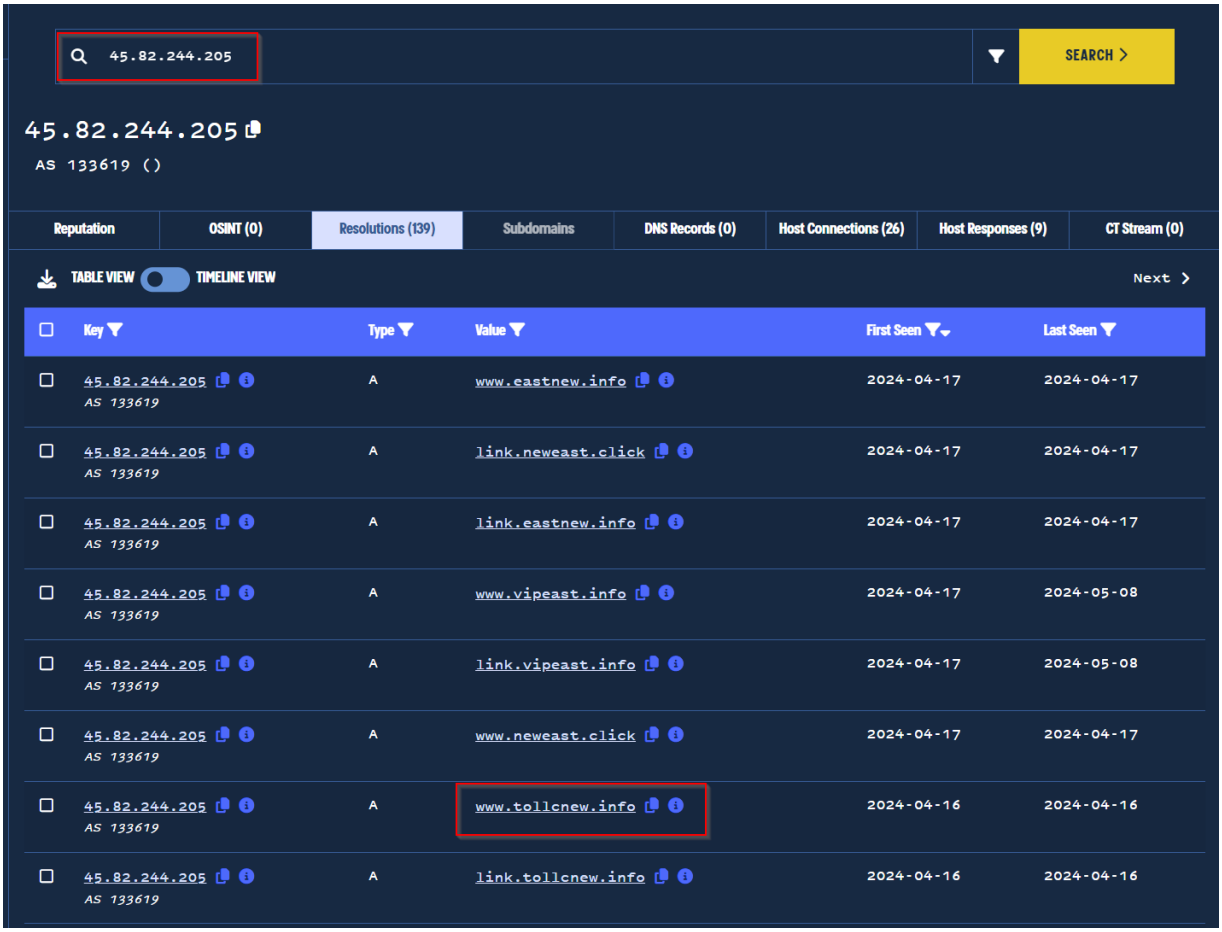
Using the lookalike search to find domains with similar naming schemes.

The results of our lookalike search revealed new domains from which we could pivot, ultimately leading to a new IP address of `45.82.244[.]205`.

This IP was first associated with toll-related domains on `2024-04-14`, which fits nicely into the timeframe from our initial analysis.

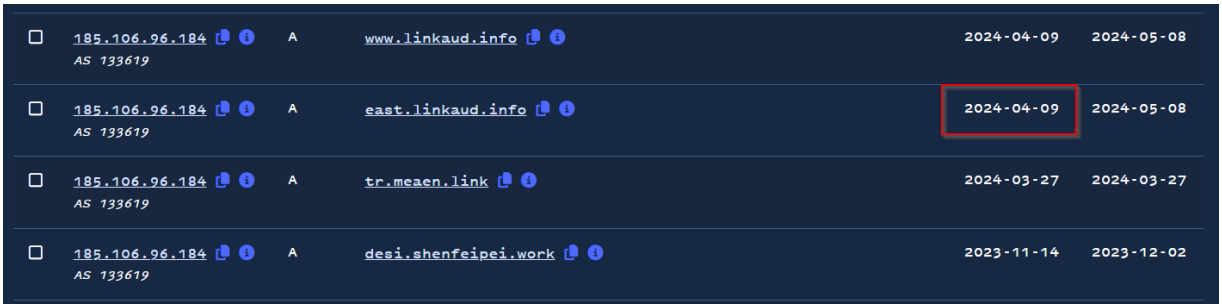
PDNS history from lookalike match shows likely-related domain.

We performed passive DNS lookups on the new `45.82.244[.]205` address. This identified 139 related domains, with 98 featuring the same toll and link themes as the initial indicator.



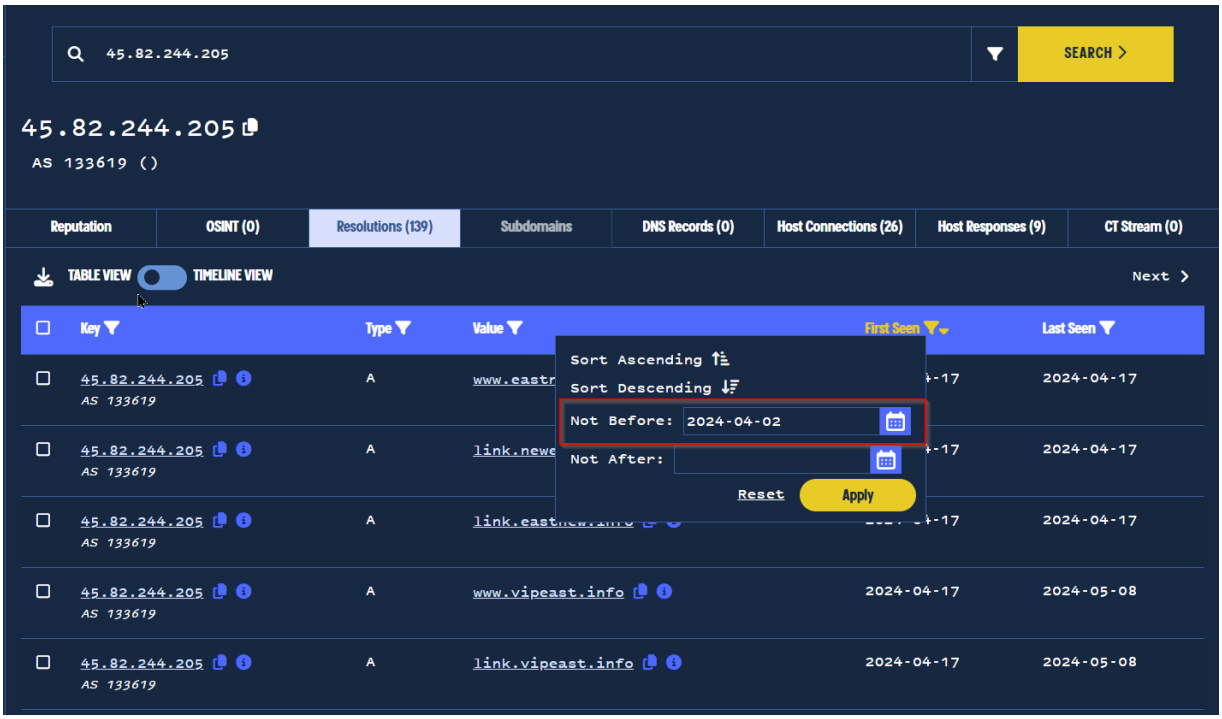
PDNS pivoting identifies 98 new toll-themed domains.

The earliest of the new domains were first seen on `2024-04-03`, which again fits into the timeframe of our previous analysis.



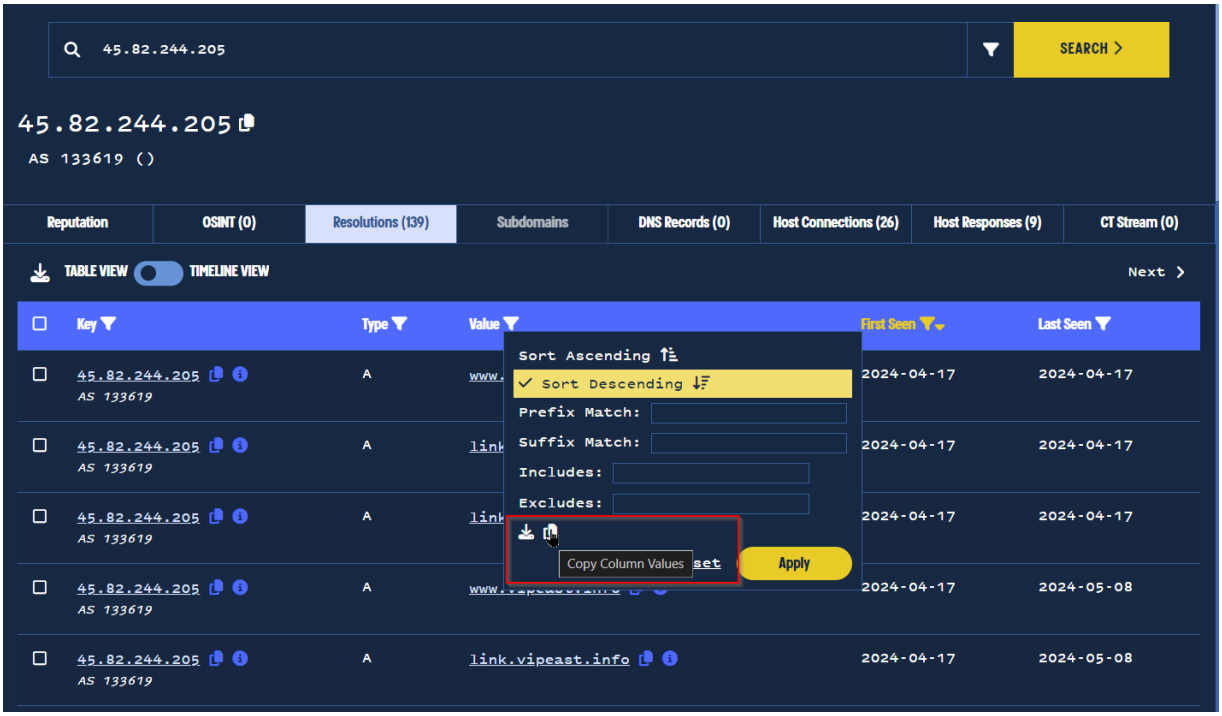
Hosting history for IP address strengthens conviction that domains are related.

There were ~40 domains prior to this date that were unrelated to toll themes, so applied a `Not Before` filter of `2024-04-02` to match the earliest observed toll domain and filter out unrelated results.



Using the Not Before filter to remove unrelated activity from results.

With the unrelated results now excluded, we could copy our domain column (now containing only the 98 related domains) and add them to our final list domain IOC's.



Copying the results to add to IOC list.

We exported the final list into CyberChef and filtered the results to determine that we had now extracted a total of 226 unique domains and 112 unique apex domains with Toll-related themes.

The final results of our search can be found below.

Final IOC List

45.82.244[.]205
91.92.251[.]193
185.106.96[.]184

east.linkacn[.]info
east.linkanew[.]info
east.linkaud[.]info
east.linkauf[.]info
east.linkauh[.]info
east.linkaui[.]info
east.linkauj[.]info
east.linkaul[.]info
east.linkauo[.]info
east.linkaup[.]info
east.linkaur[.]info
east.linkauu[.]info
east.linkauy[.]info
east.linkccm[.]info
east.linkccn[.]info
east.linkcnew[.]info
east.linkdau[.]info
east.linkiau[.]info
east.linkicm[.]info
east.linklau[.]info
east.linklcn[.]info
east.linkncn[.]info
east.linkrau[.]info
east.linksau[.]info
east.linkscn[.]info
east.linksnew[.]info
east.linktaa[.]info
east.linktae[.]info
east.linkuau[.]info
east.linkucn[.]info
east.linkvcn[.]info
east.linkvnew[.]info
east.linkxau[.]click
east.linkxau[.]info
east.linkxcm[.]info
east.linkxnew[.]info
east.linkxus[.]info
east.linkzcm[.]info
east.linkznew[.]info
east.linkzus[.]info
east.tollausc[.]info
east.tollausn[.]info
east.tollauso[.]info
east.tollausz[.]info
east.tollscau[.]info
east.tollsi[.]info
east.tollsl[.]click
east.tollsnau[.]info

east.tollsrau[.]info
east.tollsvau[.]info
east.tollsz[.]info
link.eastau[.]click
link.eastaus[.]info
link.eastnew[.]info
link.neweast[.]click
link.neweast[.]info
link.tollcnew[.]click
link.tollcnew[.]info
link.tollmau[.]info
link.tollsmau[.]info
link.tollsxau[.]info
link.vipeast[.]info
links.eastlinkau[.]click
links.eastlinkc[.]click
links.tollaau[.]info
links.tollcau[.]info
links.tolleau[.]info
links.tollgau[.]info
links.tolliau[.]info
links.tollnau[.]click
links.tollseau[.]info
links.tollslau[.]info
links.tollsuau[.]info
links.tollswau[.]info
links.tolltau[.]info
links.tolluau[.]click
links.tolluau[.]info
links.tollvau[.]info
links.tollwau[.]info
links.tollzau[.]click
links.tollzau[.]info
new.eastaun[.]click
new.eastaun[.]info
new.eastauz[.]click
new.eastauz[.]info
new.tollaug[.]info
new.tollauj[.]info
new.tollaul[.]info
new.tollaun[.]info
new.tollaus[.]info
new.tollausa[.]info
new.tollauu[.]info
new.tollaux[.]info
new.tollsa[.]click
new.tollsaua[.]info
new.tollsaui[.]info
new.tollsaum[.]click
new.tollsauu[.]click
new.tollsauu[.]info
new.tollsauv[.]info

new.tollsc[.]click
new.tollsd[.]click
new.tollsi[.]info
new.tollsl[.]click
new.tollsn[.]click
new.tollso[.]info
new.tollsr[.]click
new.tollsusc[.]info
new.tollsusu[.]info
new.tollsusw[.]info
new.tollsw[.]click
new.tollsy[.]click
tolls.eastlinkl[.]click
tolls.eastlinks[.]click
www.eastau[.]click
www.eastaun[.]click
www.eastaun[.]info
www.eastaus[.]info
www.eastauz[.]click
www.eastauz[.]info
www.eastlinkau[.]click
www.eastlinkc[.]click
www.eastlinkl[.]click
www.eastlinks[.]click
www.eastnew[.]info
www.linkacn[.]info
www.linkanew[.]info
www.linkaud[.]info
www.linkauf[.]info
www.linkauh[.]info
www.linkaui[.]info
www.linkauj[.]info
www.linkaul[.]info
www.linkauo[.]info
www.linkaup[.]info
www.linkaur[.]info
www.linkauu[.]info
www.linkauy[.]info
www.linkccm[.]info
www.linkccn[.]info
www.linkcnew[.]info
www.linkdau[.]info
www.linkiau[.]info
www.linkicm[.]info
www.linklau[.]info
www.linklcn[.]info
www.linkncn[.]info
www.linkrau[.]info
www.linksau[.]info
www.linkscn[.]info
www.linksnew[.]info
www.linktaa[.]info

www.linktae[.]info
www.linkuau[.]info
www.linkucn[.]info
www.linkvcn[.]info
www.linkvnew[.]info
www.linkxau[.]click
www.linkxau[.]info
www.linkxcm[.]info
www.linkxnew[.]info
www.linkxus[.]info
www.linkzcm[.]info
www.linkznew[.]info
www.linkzus[.]info
www.neweast[.]click
www.neweast[.]info
www.tollaau[.]info
www.tollaug[.]info
www.tollauj[.]info
www.tollaul[.]info
www.tollaun[.]info
www.tollaus[.]info
www.tollausa[.]info
www.tollausc[.]info
www.tollausn[.]info
www.tollauso[.]info
www.tollausz[.]info
www.tollauu[.]info
www.tollaux[.]info
www.tollcau[.]info
www.tollcnew[.]click
www.tollcnew[.]info
www.tolleau[.]info
www.tollgau[.]info
www.tolliau[.]info
www.tollmau[.]info
www.tollnau[.]click
www.tollsa[.]click
www.tollsaua[.]info
www.tollsaui[.]info
www.tollsaum[.]click
www.tollsauu[.]click
www.tollsauu[.]info
www.tollsauv[.]info
www.tollsc[.]click
www.tollscau[.]info
www.tollsd[.]click
www.tollseau[.]info
www.tollsi[.]info
www.tollsl[.]click
www.tollslau[.]info
www.tollsmau[.]info
www.tollsn[.]click

```
www.tollsnau[.]info
www.tollso[.]info
www.tollsr[.]click
www.tollsrau[.]info
www.tollsuau[.]info
www.tollsusc[.]info
www.tollsusu[.]info
www.tollsusw[.]info
www.tollsvau[.]info
www.tollsw[.]click
www.tollswau[.]info
www.tollsxau[.]info
www.tollsy[.]click
www.tollsz[.]info
www.tolltau[.]info
www.tolluau[.]click
www.tolluau[.]info
www.tollvau[.]info
www.tollwau[.]info
www.tollzau[.]click
www.tollzau[.]info
www.vipeast[.]info
```

Apex Domains

eastau[.]click
eastaun[.]click
eastaun[.]info
eastaus[.]info
eastauz[.]click
eastauz[.]info
eastlinkau[.]click
eastlinkc[.]click
eastlinkl[.]click
eastlinks[.]click
eastnew[.]info
linkacn[.]info
linkanew[.]info
linkaud[.]info
linkauf[.]info
linkauh[.]info
linkaui[.]info
linkauj[.]info
linkaul[.]info
linkauo[.]info
linkaup[.]info
linkaur[.]info
linkauu[.]info
linkauy[.]info
linkccm[.]info
linkccn[.]info
linkcnew[.]info
linkdau[.]info
linkiau[.]info
linkicm[.]info
linklau[.]info
linklcn[.]info
linkncn[.]info
linkrau[.]info
linksau[.]info
linkscn[.]info
linksnew[.]info
linktaa[.]info
linktae[.]info
linkuau[.]info
linkucn[.]info
linkvcn[.]info
linkvnew[.]info
linkxau[.]click
linkxau[.]info
linkxcm[.]info
linkxnew[.]info
linkxus[.]info
linkzcm[.]info
linkznew[.]info
linkzus[.]info
neweast[.]click

neweast[.]info
tollaau[.]info
tollaug[.]info
tollauj[.]info
tollaul[.]info
tollaun[.]info
tollaus[.]info
tollausa[.]info
tollausc[.]info
tollausn[.]info
tollauso[.]info
tollausz[.]info
tollauu[.]info
tollaux[.]info
tollcau[.]info
tollcnew[.]click
tollcnew[.]info
tolleau[.]info
tollgau[.]info
tolliau[.]info
tollmau[.]info
tollnau[.]click
tollsa[.]click
tollsaua[.]info
tollsaui[.]info
tollsaum[.]click
tollsauu[.]click
tollsauu[.]info
tollsauv[.]info
tollsc[.]click
tollscau[.]info
tollsd[.]click
tollseau[.]info
tollsi[.]info
tollsl[.]click
tollslau[.]info
tollsmau[.]info
tollsn[.]click
tollsnau[.]info
tollso[.]info
tollsr[.]click
tollsrau[.]info
tollsuau[.]info
tollsusc[.]info
tollsusu[.]info
tollsusw[.]info
tollsvau[.]info
tollsw[.]click
tollswau[.]info
tollsxau[.]info
tollsy[.]click
tollsz[.]info

```
tolltau[.]info
tolluau[.]click
tolluau[.]info
tollvau[.]info
tollwau[.]info
tollzau[.]click
tollzau[.]info
vipeast[.]info
```

Conclusion

Interested in leveraging Validin to build high-confidence, custom threat intelligence? Check out our individual pricing and plans, or contact us to learn about our enterprise options.

Eliminate blind spots with comprehensive DNS history.

Contact us for a demo