Introduction To Malware Infrastructure Analysis With Passive DNS

By Matthew

Published: 2024-03-27 · Archived: 2026-04-02 12:01:50 UTC

We recently became aware of an awesome DNS Analysis tool called Validin which can be used to analyse malicious domains and show related infrastructure using DNS records.

This has been super useful as existing infrastructure analysis tools are primarily focused on analysis and pivoting from IPs, which functions very differently to pivoting from domains.

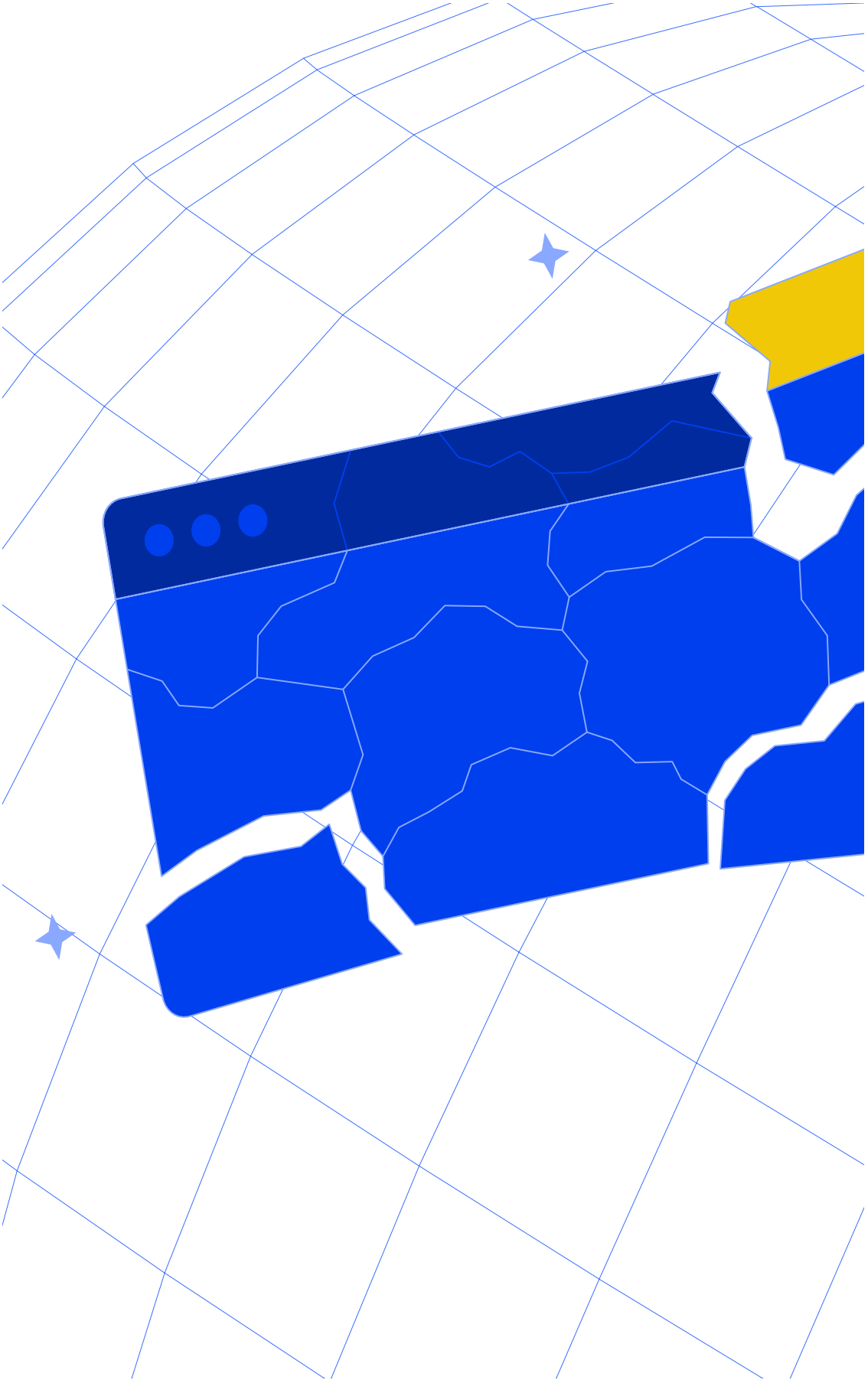
The primary concept of DNS pivots is simple, use the DNS history and domain names to identify patterns and related indicators which threat actors have re-used when deploying infrastructure.

Since we're having a lot of fun with the tool and the techniques, we wanted to share some cool and useful examples that we have encountered so far.

You can follow along with the free community version available here.

> Validin
>
> Validin offers cutting-edge DNS, certificate, and crawling data services to empower threat researchers and corporate security teams. Identify, track, and mitigate risks with our advanced threat intelligence solutions.

Validin

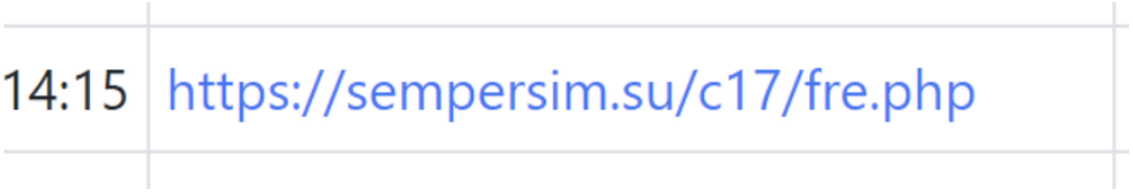


Practical Use Cases

- Identifying the history of a domain (Current and Previous IP's)
- Finding lookalike domains with similar names
- Identifying domains that resolve to the same IP
- Identifying domains with a similar parent domain (.duckdns.org, .ddns etc)

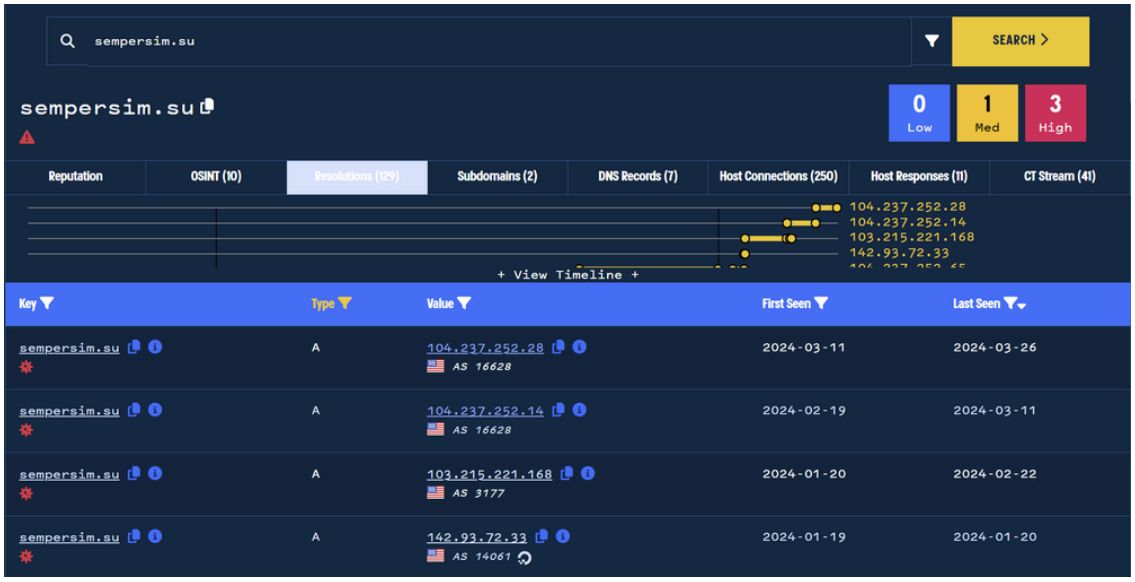
LokiBot - Identifying IP History

As an initial example using Validin, we can take this domain which was reported as Lokibot on ThreatFox.



By searching for this domain `sempersim[.]su` , we can obtain a full history of IP infrastructure related to this domain.

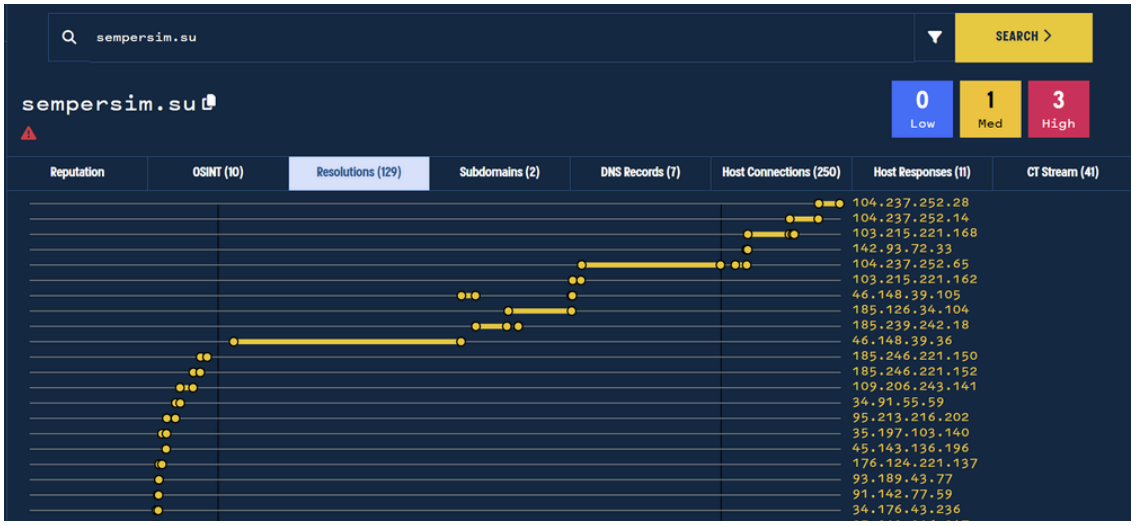
(A link to this search can be found here and followed with a free account)



There are a large number of IPs associated with this domain. The first is from 2022 and has constantly changed since then.

This is an indicator that the actor is regularly changing up their infrastructure, possibly in response to intel sharing or takedowns.

This can be better visualized in the timeline feature demonstrated below. Many of the IPs are short-lived, and some have lasted longer than others.



LokiBot - Identifying Related Domains

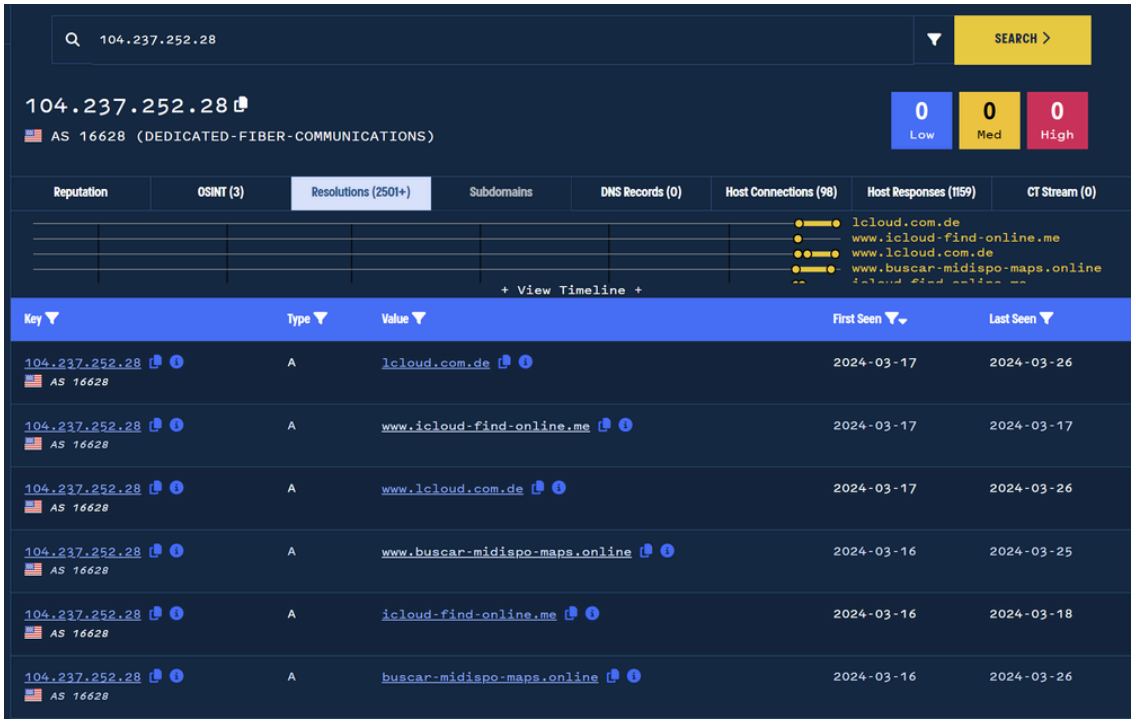
In the initial search on our `sempersim[.]su` domain, the most recently added result was an IP address of `104.237.252[.]28`.

We can do a pivot on this IP address and view the history of related domains, this allows us to identify additional domains which have resolved to the same server as `sempersim[.]su`

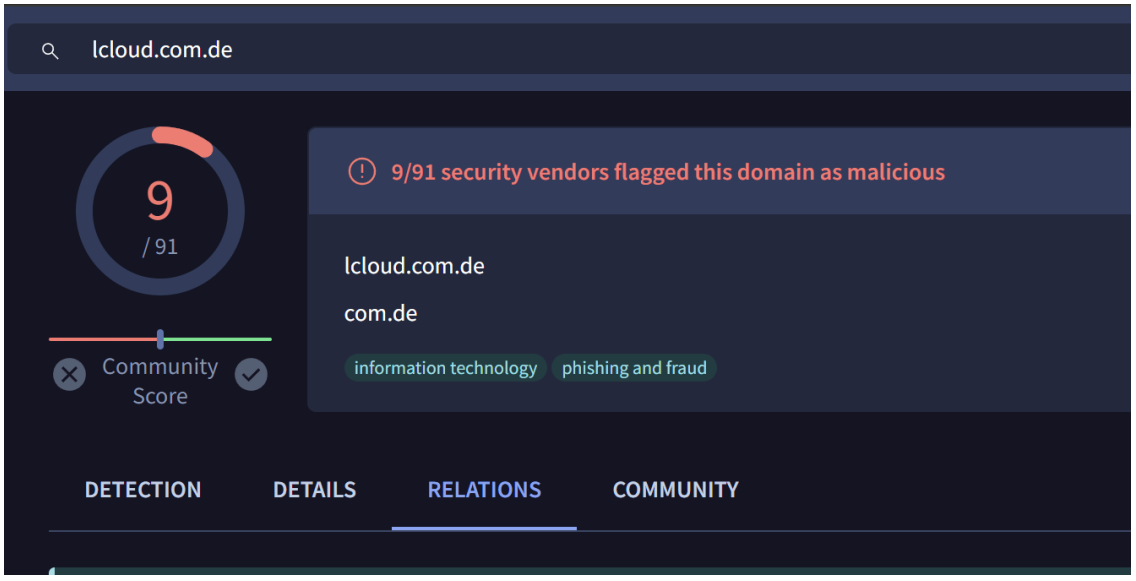
By searching or clicking on `104.237.252[.]28`, we can pivot on this IP and see if there are any recent domains pointing to the same location.

In this case, there are 6 domains that have been pointing at this address in the 2 weeks prior to this analysis.

Four of these results seem to be impersonating Icloud services (Using L instead of I).



The resulting domains can be investigated and validated with other tooling, here is one such example of the first related domain `lcloud.com[.]de` in Virustotal.



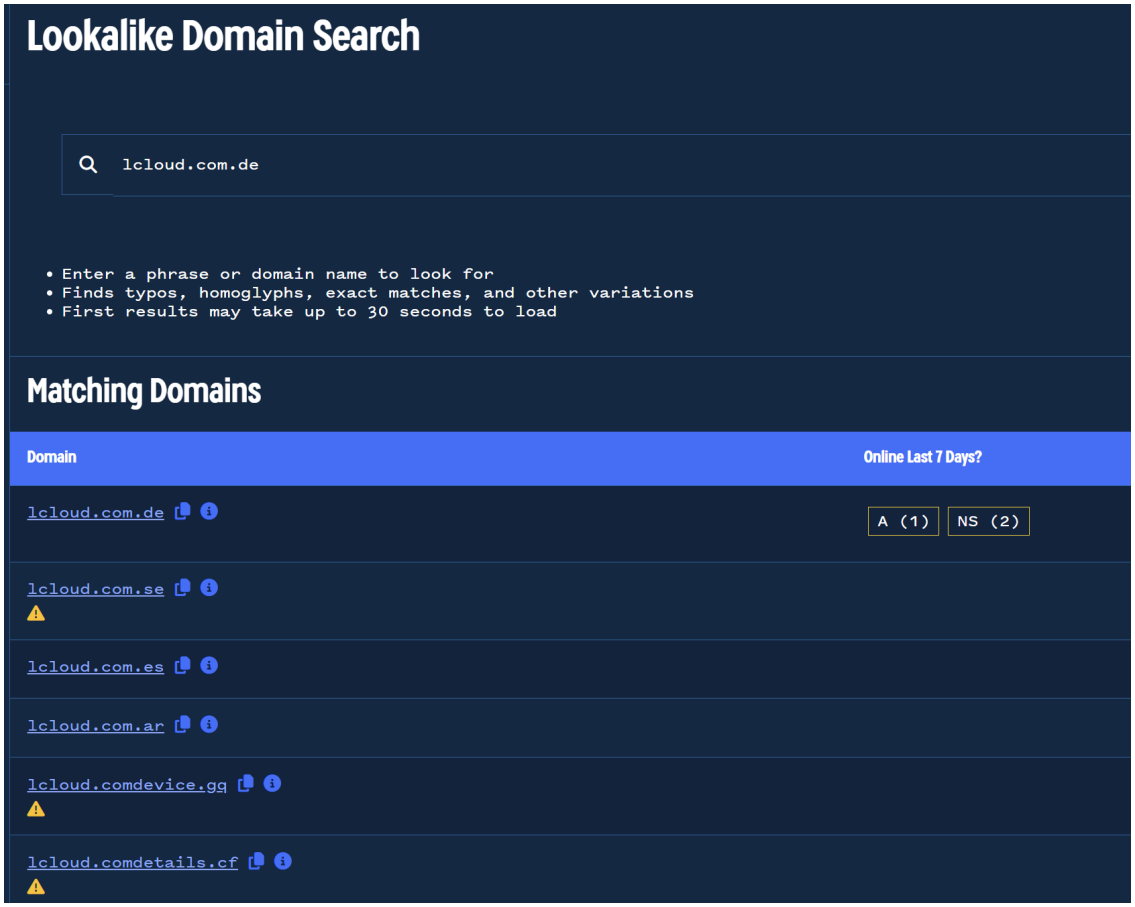
The remaining results are highly suspicious and are likely related to the same actor as the initial `sempersim[.]su` domain.

Identifying LookAlike Domains

The previous analysis pivoted from `sempersim[.]su` to identify a new domain of `lcloud.com[.]de` (L instead of I).

This new indicator is highly suspicious as it appears to be impersonating an Apple icloud service.

If an actor is utilising one fake ICloud domain, they potentially have more using the same technique. We can validate this theory using the lookalike domain feature on the `lcloud.com[.]de` domain.

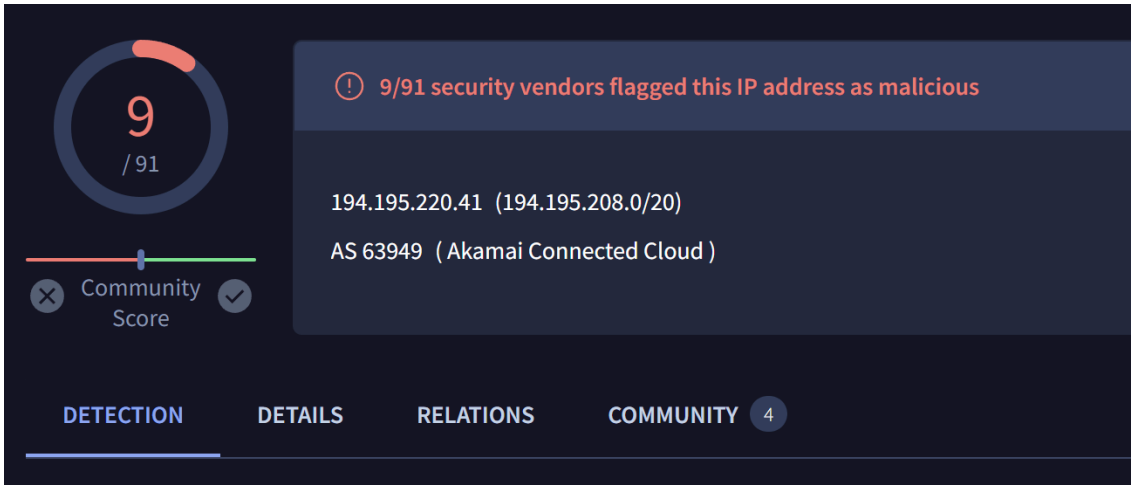


This search returns 1033 total results for domains with the same mispelling, but for the purposes of demonstration, we will use the first new result of `lcloud.com[.]se`.

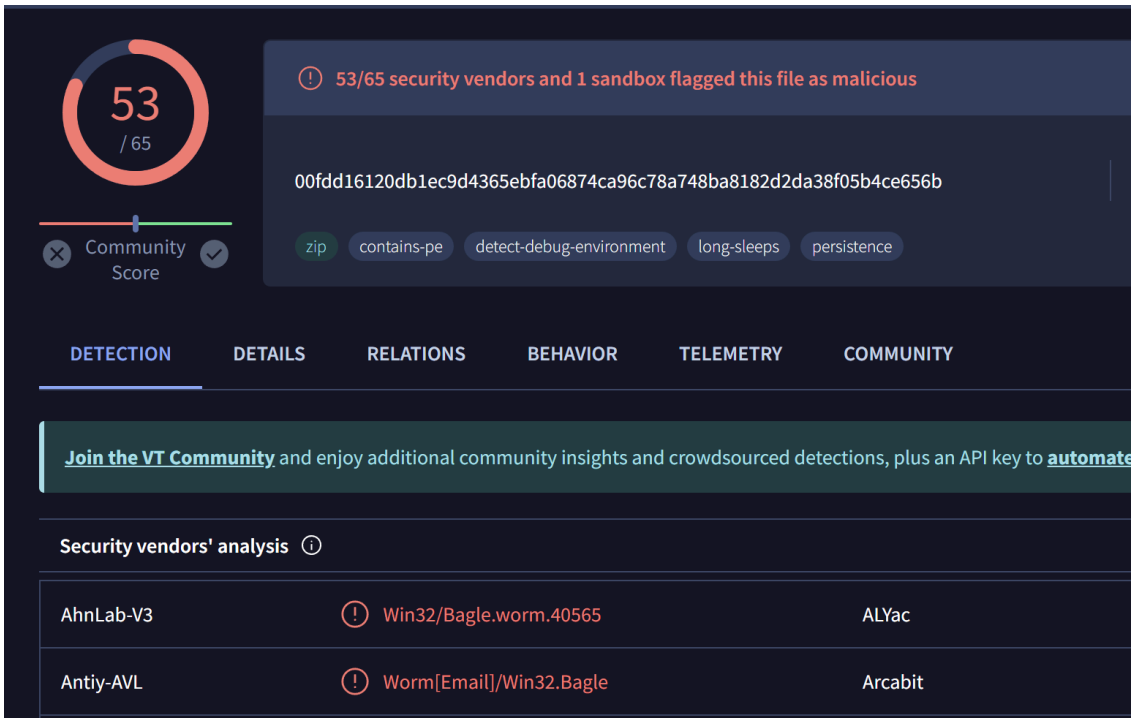
Pivoting on this new `.se` domain reveals a history of 15 IP addresses ranging from 2019 to 2023.

Key	Type	Value	First Seen	Last Seen
lcloud.com.se	A	194.195.220.41 AS 63949	2023-11-16	2023-11-28
lcloud.com.se	A	95.46.8.229 AS 44546	2022-11-22	2023-02-20
lcloud.com.se	A	172.67.155.153 AS 13335	2022-10-16	2022-11-21
lcloud.com.se	A	104.21.80.241 AS 13335	2022-10-16	2022-11-21

The most recent (based on first seen) of these ip addresses is `194.295.220[.]41`, initial analysis of this IP with Virustotal reveals 9 related detections.



Review of the communicating files for this IP reveals multiple files related to the "Bagle Worm"

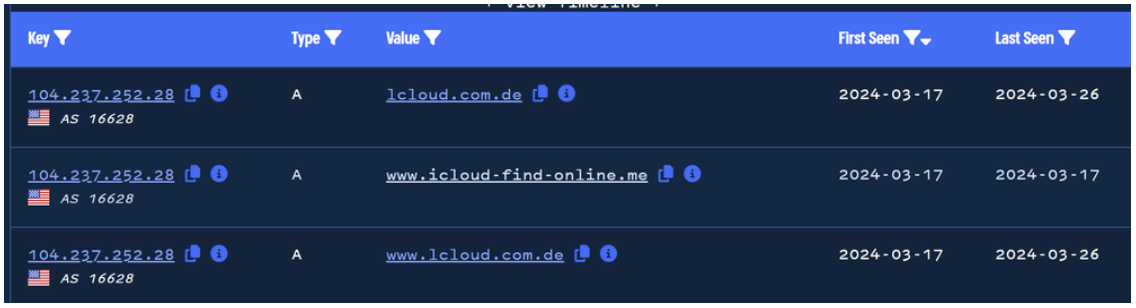


We are not particularly familiar with Bagle, but at first glance it seems wildly different to the initial indicator which was based on LokiBot.

This could be an indicator that the actors behind Lokibot and Bagle are sharing the same infrastructure, or could be an indicator that they are the same actor.

Exact attribution is beyond the scope of this post, but it's an interesting note that the two are potentially sharing infrastructure or at least leveraging extremely similar domains.

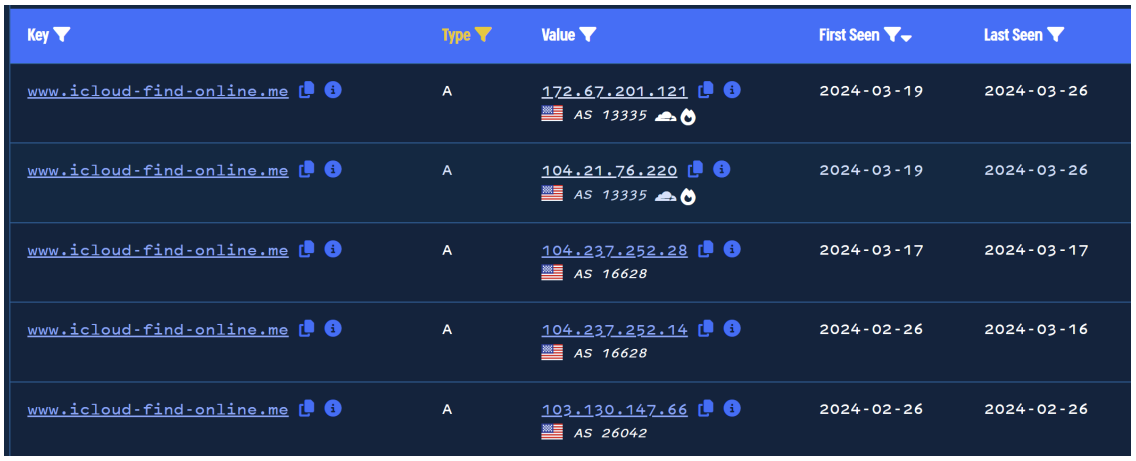
Returning to our pivot on `sempersim[.]su`, we identified an IP address of `104.237.252[.]28` which is also related to `www.icloud-find-online[.]me`.



Key	Type	Value	First Seen	Last Seen
104.237.252.28 AS 16628	A	lcloud.com.de	2024-03-17	2024-03-26
104.237.252.28 AS 16628	A	www.icloud-find-online.me	2024-03-17	2024-03-17
104.237.252.28 AS 16628	A	www.lcloud.com.de	2024-03-17	2024-03-26

By pivoting to this new domain `www.icloud-find-online[.]me`, we can see the full history of IPs related to the domain.

By observing the ASN numbers and the presence of the "cloud" symbol next to the ASN, we can see that the actor behind this domain began to use CloudFlare as of `2024-03-19`

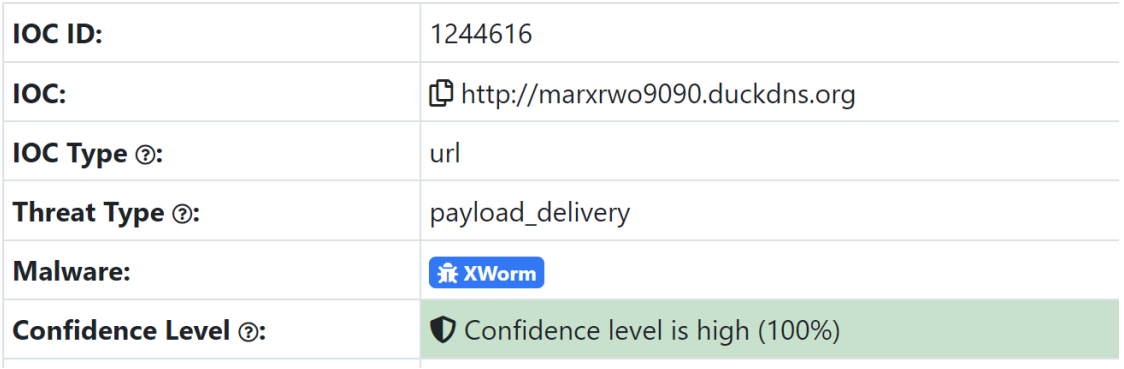


Key	Type	Value	First Seen	Last Seen
www.icloud-find-online.me	A	172.67.201.121 AS 13335	2024-03-19	2024-03-26
www.icloud-find-online.me	A	104.21.76.220 AS 13335	2024-03-19	2024-03-26
www.icloud-find-online.me	A	104.237.252.28 AS 16628	2024-03-17	2024-03-17
www.icloud-find-online.me	A	104.237.252.14 AS 16628	2024-02-26	2024-03-16
www.icloud-find-online.me	A	103.130.147.66 AS 26042	2024-02-26	2024-02-26

This isn't particularly useful to me, but seeing it visualized like this is cool. More experienced intel analysts may have plenty of use for this information.

Xworm - Identifying Related Domains

Here we have another highly suspicious domain name `marxrwo9090.duckdns[.]org` which was reported as Xworm on ThreatFox.



IOC ID:	1244616
IOC:	http://marxrwo9090.duckdns.org
IOC Type ⓘ:	url
Threat Type ⓘ:	payload_delivery
Malware:	XWorm
Confidence Level ⓘ:	Confidence level is high (100%)

By analysing this domain, we can see that only a single IP of `194.147.140[.]138` has been associated.

Key	Type	Value	First Seen	Last Seen
marxrwo9090.duckdns.org	NX		2024-03-05	2024-03-27
marxrwo9090.duckdns.org	A	194.147.140.138 AS 208476	2024-03-05	2024-03-27

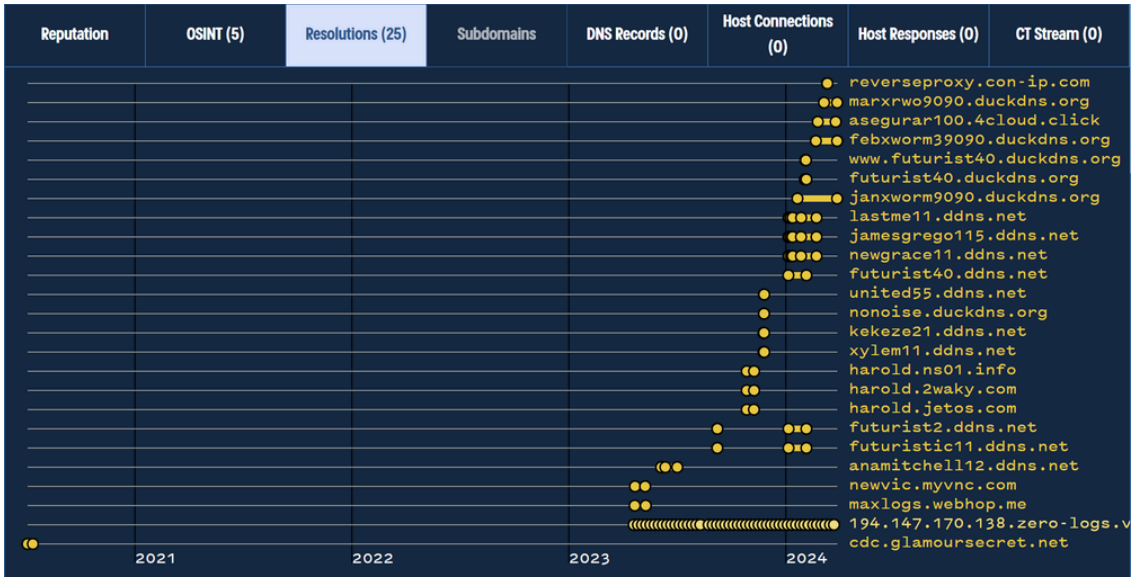
By pivoting on this IP address, we can identify a number of suspicious `.duckdns.org` domains pointing to the same location.

One of these results specifically calls out Xworm as `febxworm39090.duckdns[.]org`

Key	Type	Value	First Seen	Last Seen
194.147.140.138 AS 208476	A	reverseproxy.con-ip.com	2024-03-10	2024-03-10
194.147.140.138 AS 208476	A	marxrwo9090.duckdns.org	2024-03-05	2024-03-27
194.147.140.138 AS 208476	A	asegurar100.4cloud.click	2024-02-23	2024-03-24
194.147.140.138 AS 208476	A	febxworm39090.duckdns.org	2024-02-20	2024-03-27
194.147.140.138 AS 208476	A	www.futurist40.duckdns.org	2024-02-02	2024-02-03
194.147.140.138 AS 208476	A	futurist40.duckdns.org	2024-02-01	2024-02-04

There are 25 domains associated with the address `194.147.140[.]138`, and we can again visualise these with the timeline feature.

Here, we can see the actor has regularly updated their domains and has primarily relied on dynamic DNS services such as ddns and duckdns.



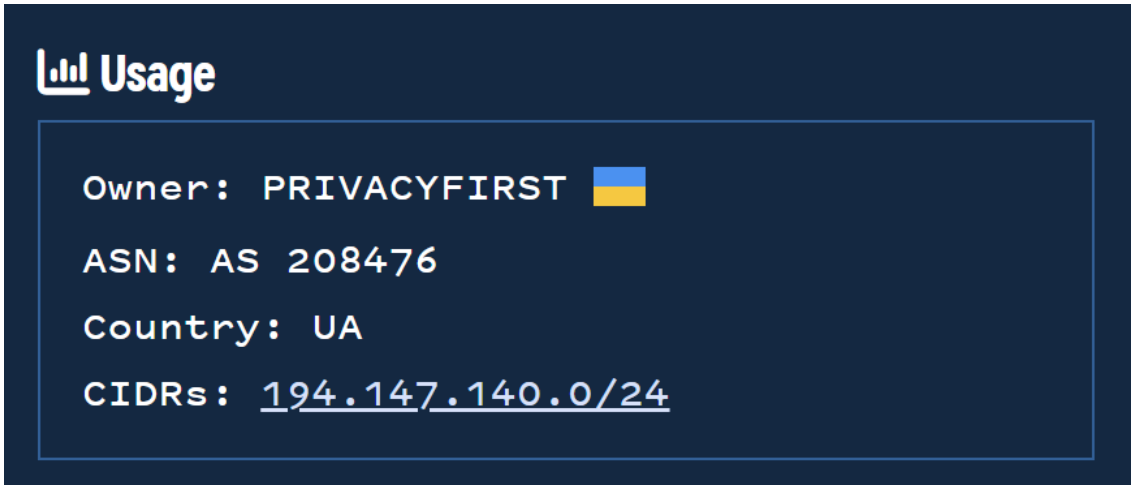
Xworm - Pivoting Across CIDR Ranges

In the previous section, we identified that the actor was regularly using dynamic DNS services to mask the IP at `194.147.140[.]138`

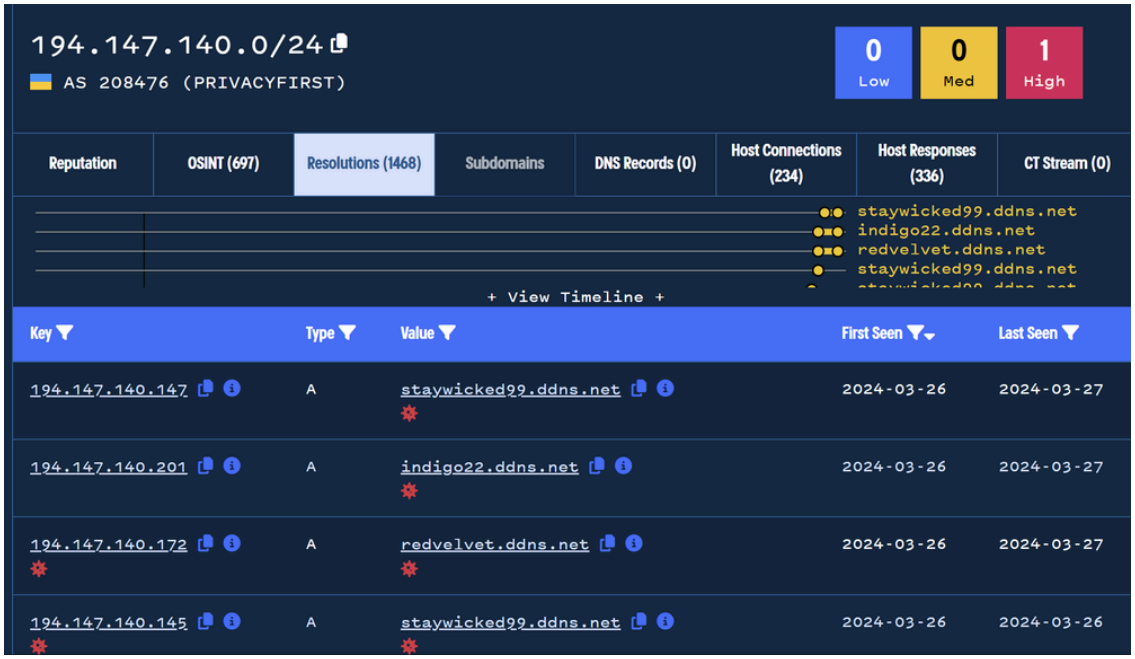
If we consider that the same actor may be using the same ASN or hosting provider to host similar infrastructure, we can craft a query to identify additional related domains.

Consider that the initial IP `194.147.140[.]138` belongs to an AS with a CIDR range `194.147.140.0/24`

(This section is similar to that published by Gi7w0rm on his DDGroup Analysis, so be sure to check that out too)



We can expand the search to query this range, which reveals 1468 domains with IP addresses resolving to the ASN. Many of these domains also rely on dynamic dns services such as `ddns` and `duckdns`.



A total of 464 domains are leveraging duckdns and resolving to the same ASN. Many of these have highly suspicious names and are very recent.

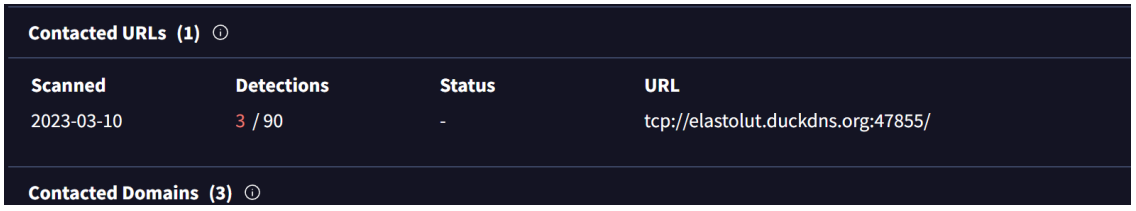
Key	Type	Value	First Seen	Last Seen
194.147.140.229	A	elastolut.duckdns.org	2024-03-21	2024-03-27
194.147.140.229	A	elastsolek.duckdns.org	2024-03-21	2024-03-27
194.147.140.229	A	zekeriyasolek45.duckdns.org	2024-03-21	2024-03-27
194.147.140.229	A	zekeriyasolek44.duckdns.org	2024-03-21	2024-03-27
194.147.140.229	A	elastsolek1.duckdns.org	2024-03-21	2024-03-27
194.147.140.141	A	ansrt.duckdns.org	2024-03-21	2024-03-27

The first of such results is `elastolut.duckdns[.]org` , which has 11 detections on Virustotal and multiple malicious (and very recent) communicating files.

Communicating Files (4)

Scanned	Detections	Type	Name
2024-02-26	64 / 72	Win32 EXE	Windows Audio Play.exe
2023-03-14	60 / 69	Win32 EXE	Windows Audio Play.exe
2023-03-14	48 / 64	ZIP	99c08d57c4ffa904bc008d6112e5a81f70cf8e273718e040574b796ae2fcc10a
2023-06-29	66 / 71	Win32 EXE	Windows Audio Play.exe

The first of these related files has been marked as Remcos and have the `elastolut.duckdns[.]org` listed as a C2

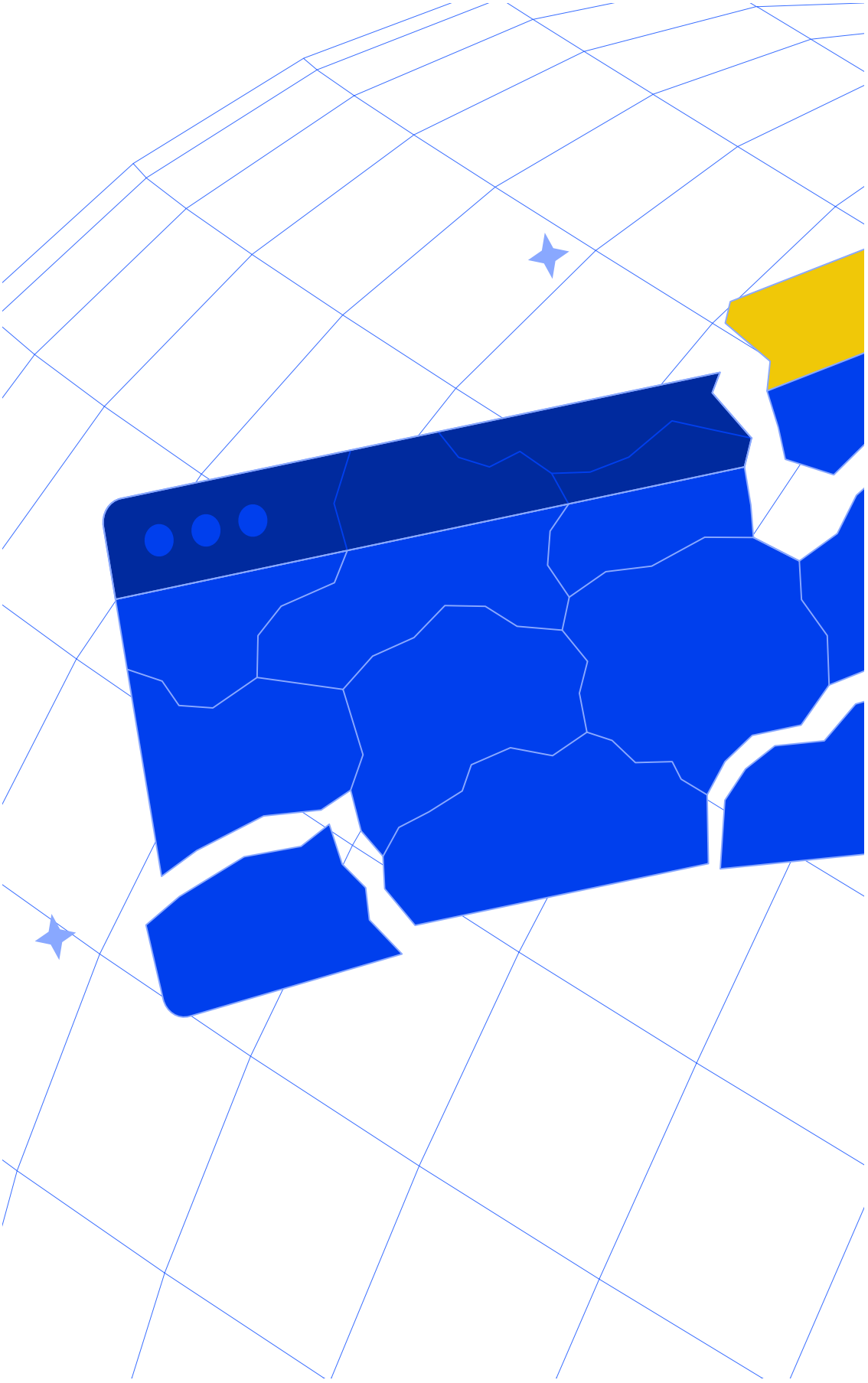


Follow Along With This Analysis

The primary tool we have used here is Validin.

> Validin even has a community (free) version for researchers to experiment with.
>
> Validin
>
> Validin offers cutting-edge DNS, certificate, and crawling data services to empower threat researchers and corporate security teams. Identify, track, and mitigate risks with our advanced threat intelligence solutions.

Validin



Sign up for Embee Research

Malware Analysis and Threat Intelligence Research

No spam. Unsubscribe anytime.

- (Joe Slowik) Stranded on Pylos - https://pylos.co/2022/11/23/detailing-daily-domain-hunting/
- A Beginners Guide to Tracking Malware Infrastructure - https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/
- (Gi7w0rm) Uncovering DDGroup - A Long Time Threat Actor
- (JoshuaPenny) **Infrastructure Analysis: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023–4966 Citrix Bleed Vulnerability**
