How To Track Malicious Infrastructure With DNS Records - Vultur Banking Trojan

By Matthew

Published: 2024-04-11 · Archived: 2026-04-06 00:04:23 UTC

Threat Actors are known for monitoring public reports and adjusting infrastructure that believe may be compromised. As intelligence analysts, it's important to be able to keep up with these changes and update intelligence queries accordingly.

In this blog, we'll examine an example in which the developers behind the Vultur banking trojan *appear* to have updated the naming scheme of their domain infrastructure in response to a public threat intelligence report.

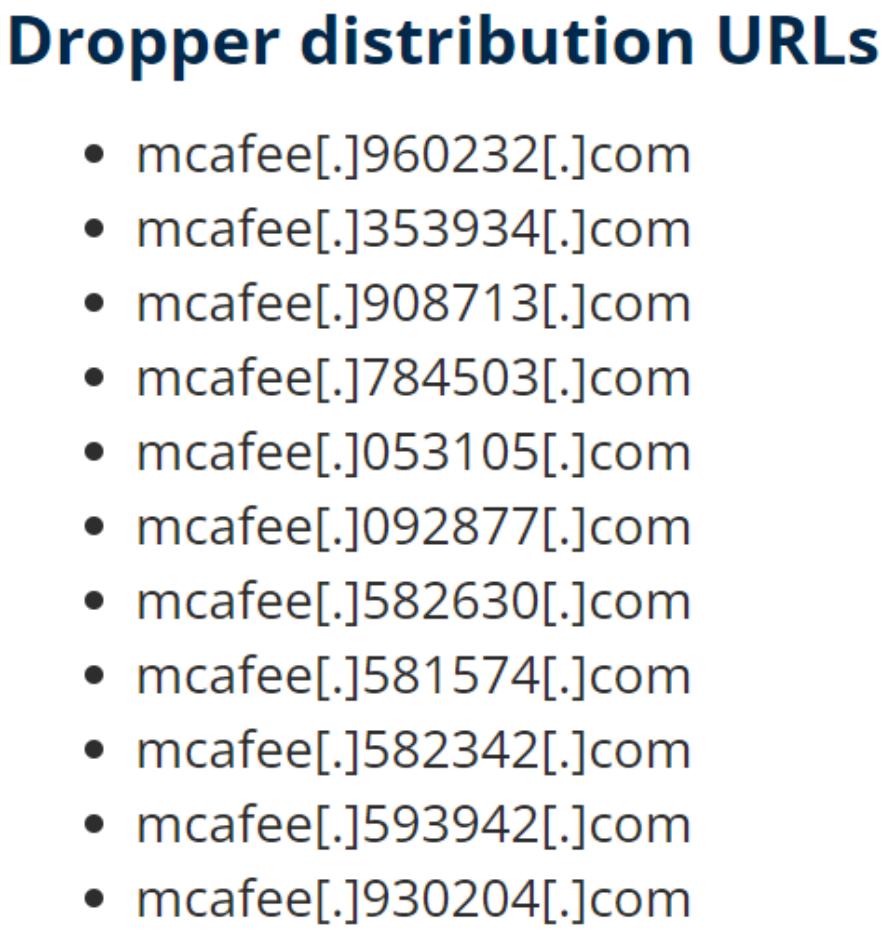
We will use passive DNS tooling to cross-examine historical domains and identify common infrastructure and patterns in naming schemes. We will leverage these as pivot points to identify 13 new domains in use by the Vultur developers.

Initial Intelligence

The initial intelligence for this post originates from a fantastic Fox-it article describing Vultur Activity. The article goes into great detail about Vultur and its capabilities.

We won't be covering the Vultur functionality here; instead, we will leverage the provided dropper distribution URLs to identify additional infrastructure.

The original dropper distribution URLs provided in the Fox-it article can be seen below.



Initial URLs provided by Fox-IT Report on Vultur

Initial Analysis Of Distribution URLs

The first step here is to gather basic intelligence on the initial reported URLs.

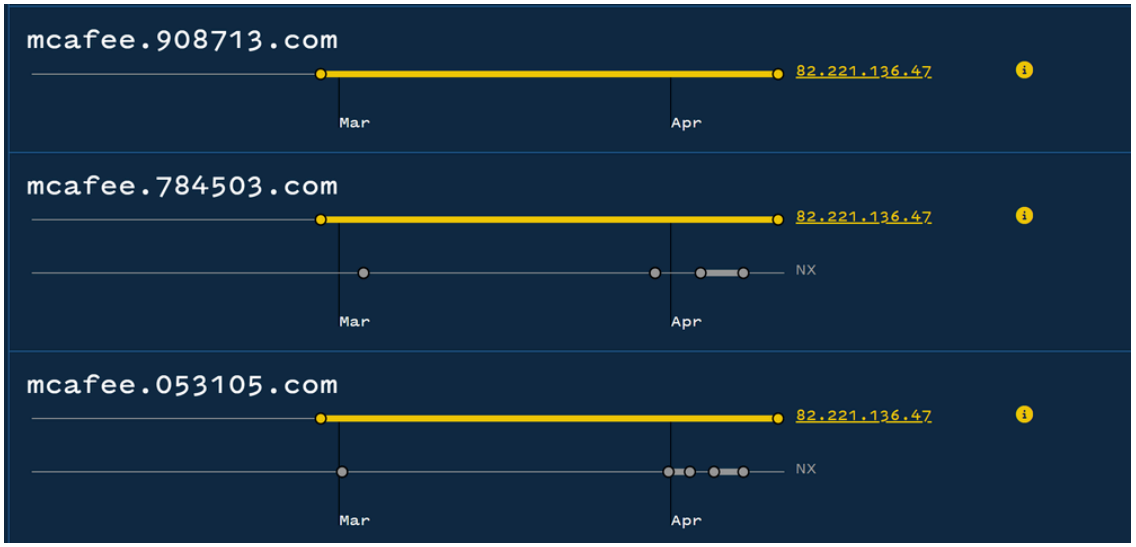
We will be leveraging Validin for this analysis. However, you are welcome to use any passive DNS tooling that you have access to.

The initial intelligence can be obtained using a bulk lookup, which provides a summary of the historical IP addresses associated with each initial domain.

We can leverage this to look for any commonalities in the historical IP addresses and establish an initial pivot point.

The bulk lookup returns the list of historical IPs for the domains, and immediately, we can see a commonality in historical IP addresses, which we can leverage as an initial pivot point.

Below we can see that several of the domains have historically resolved to the same IP address of `82.221.136[.]47`

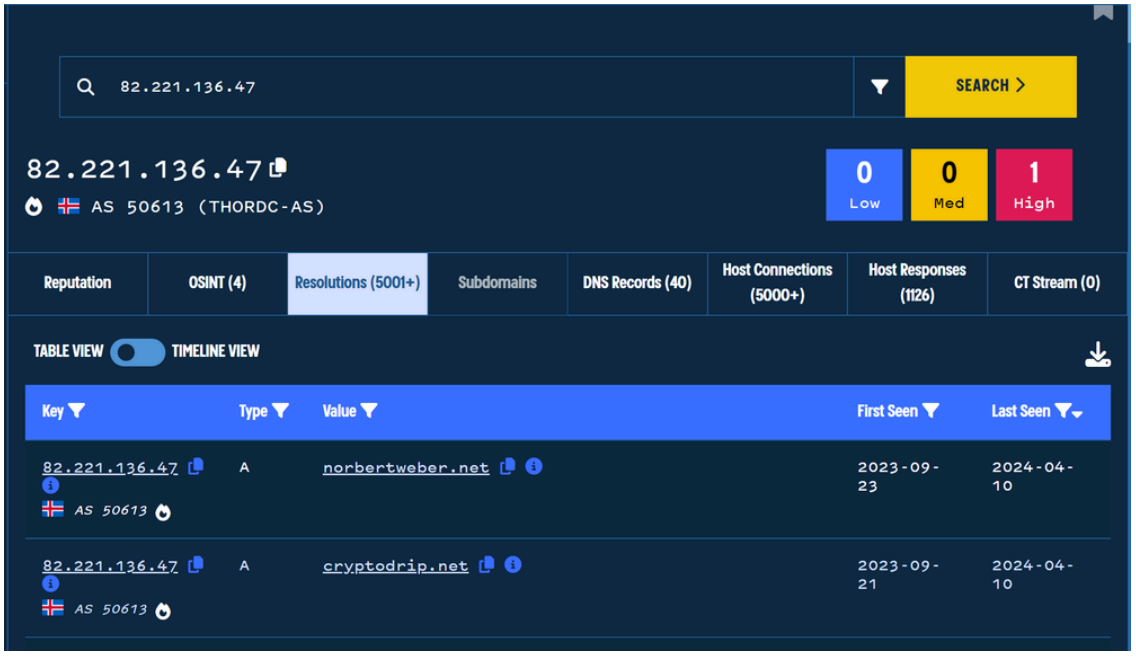


Initial Pivot on Common IP Address

With a common IP address identified across several (but not all) of the initial URLs, we can leverage this as a pivot point by searching on the IP address and viewing domains that have previously been associated.

In this case there are over 5000 domains associated. Indicating that this IP is likely a load balancer, proxy, or some kind of shared infrastructure.

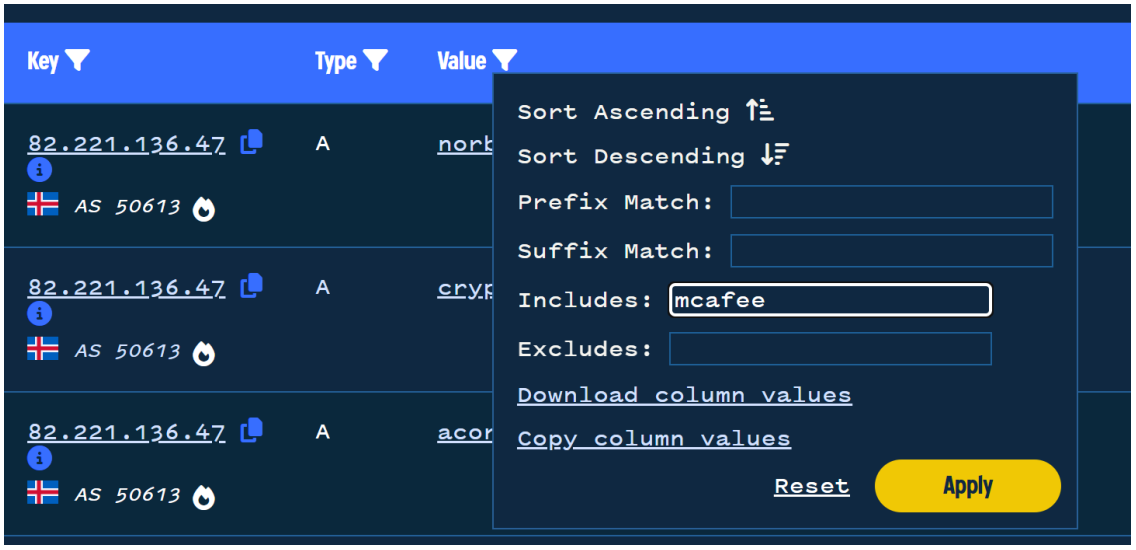
This means that the IP itself may not be malicious, but there are malicious domains routing through it.



Pivoting on Subdomain

The initial intelligence shows that the malicious domains all contain the "mcafee" subdomain.

We can leverage this to narrow down our 5000 domains to only those that contain "mcafee".

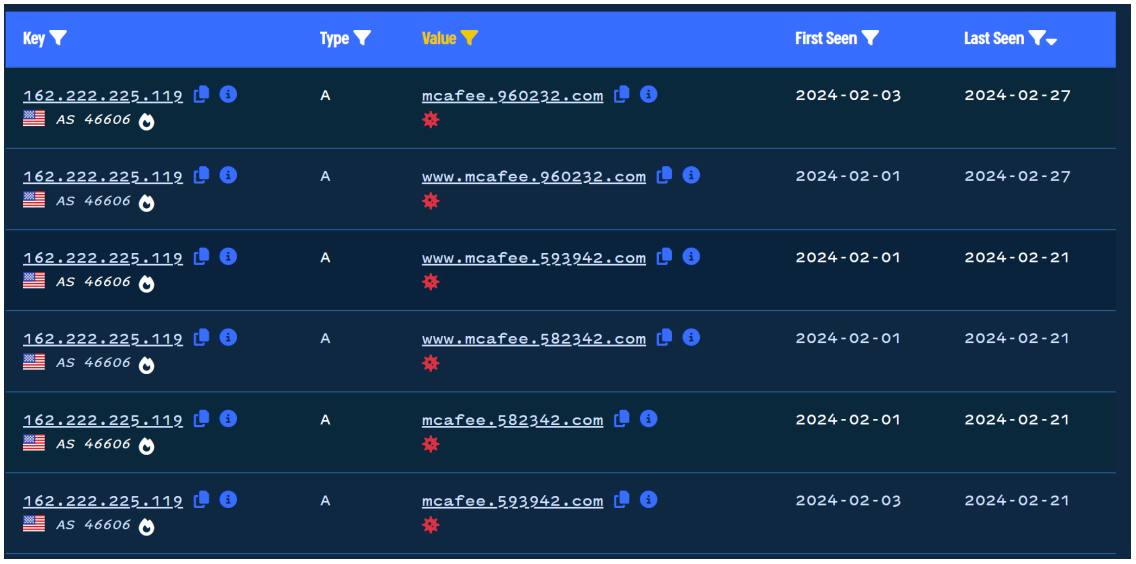


Applying the "mcafee" filter brings the 5000+ results down to only 24.

These 24 results show several of our initial domains and some new domains that leverage a hyphen between the numerical values.

Key	Type	Value	First Seen	Last Seen
82.221.136.47 AS 50613	A	mcafee.092877.com	2024-02-28	2024-04-10
82.221.136.47 AS 50613	A	mcafee.357-46.com	2024-03-08	2024-04-10
82.221.136.47 AS 50613	A	mcafee.053105.com	2024-02-28	2024-04-10
82.221.136.47 AS 50613	A	mcafee.908713.com	2024-02-28	2024-04-10
82.221.136.47 AS 50613	A	mcafee.798-13.com	2024-03-08	2024-04-10

If we repeat this process for other observed IP addresses, we can see some of the same URLs provided in the initial report.



Key	Type	Value	First Seen	Last Seen
162.222.225.119 AS 46606	A	mcafee.960232.com	2024-02-03	2024-02-27
162.222.225.119 AS 46606	A	www.mcafee.960232.com	2024-02-01	2024-02-27
162.222.225.119 AS 46606	A	www.mcafee.593942.com	2024-02-01	2024-02-21
162.222.225.119 AS 46606	A	www.mcafee.582342.com	2024-02-01	2024-02-21
162.222.225.119 AS 46606	A	mcafee.582342.com	2024-02-01	2024-02-21
162.222.225.119 AS 46606	A	mcafee.593942.com	2024-02-03	2024-02-21

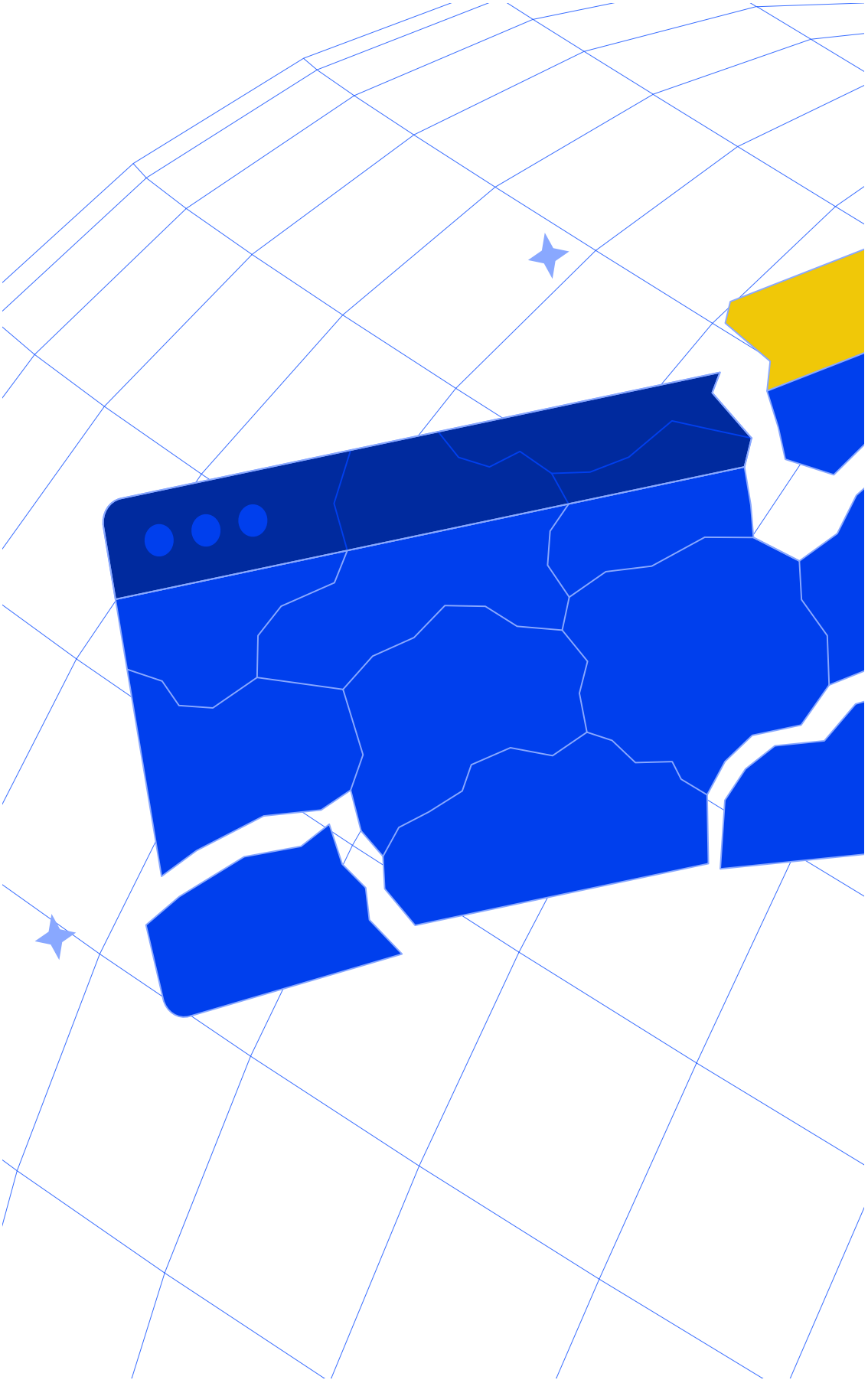
As well as some new results where the actor has increased the number of numerical values and included a hyphen.

This process can be repeated with the remainder of the IPs found in the initial bulk search. As well as with new IPs discovered in historical records during the investigation process.

During our initial review, we were able to obtain 13 domains on the same infrastructure that were not included in the initial report.

As we did not check every IP address and resolve every domain, there are likely more out there that can be found with extra searching. You are welcome to try and find more using the free Community Edition of Validin.

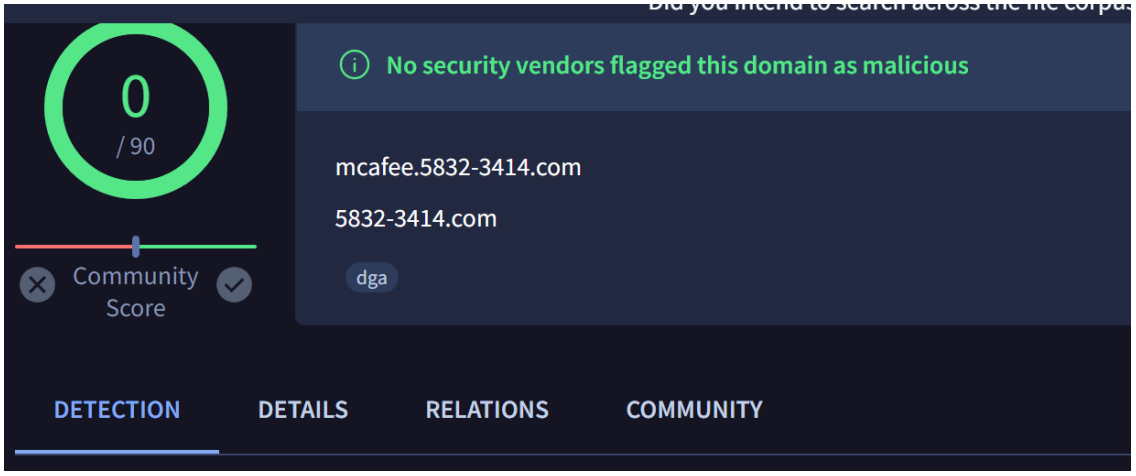
> Validin
>
> Validin offers cutting-edge DNS, certificate, and crawling data services to empower threat researchers and corporate security teams. Identify, track, and mitigate risks with our advanced threat intelligence solutions.
>
> 
>
> Validin

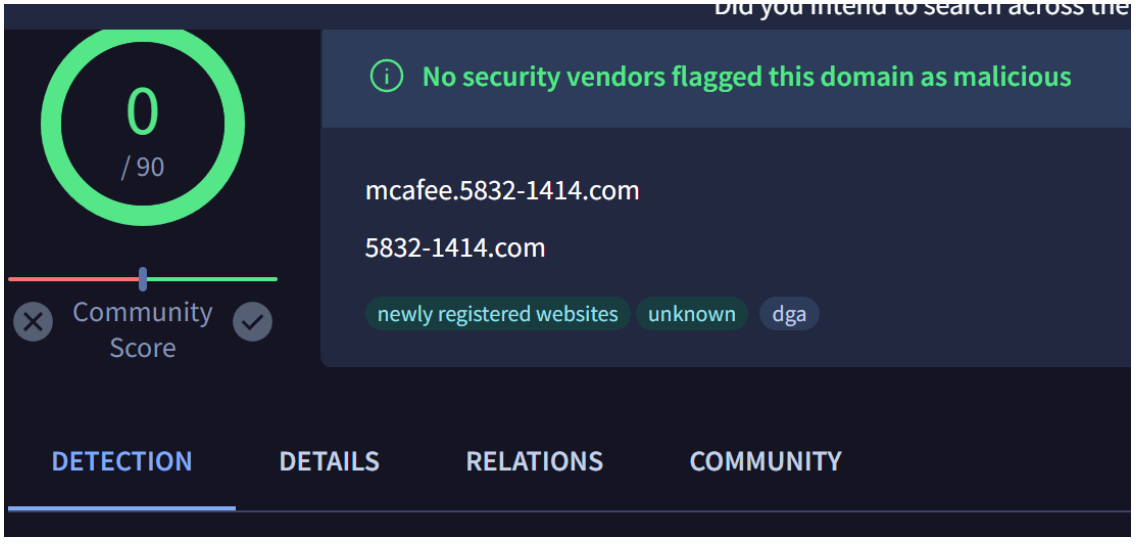


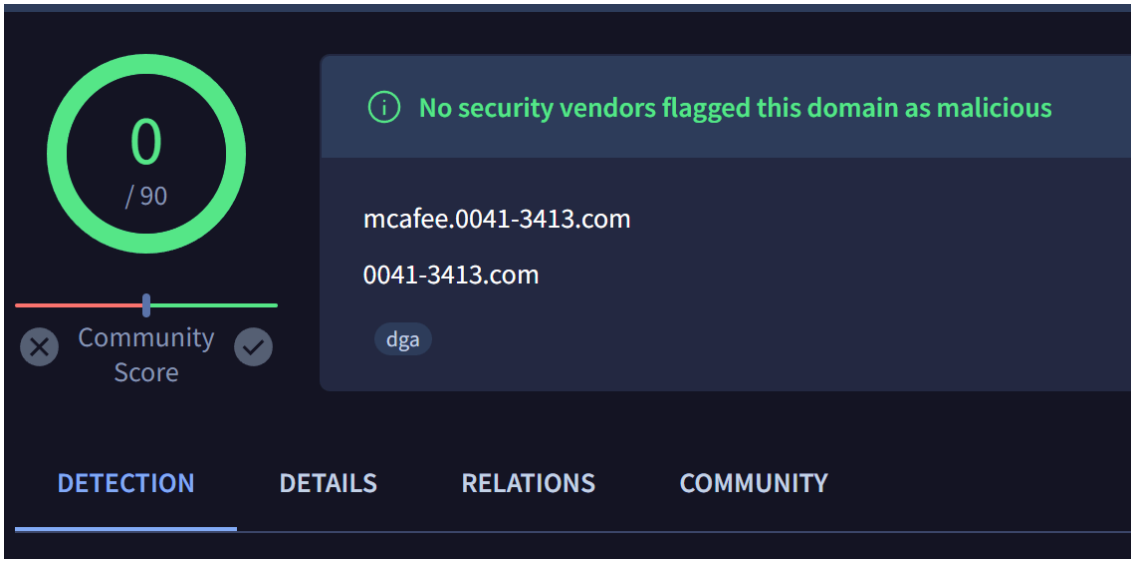
List of Malicious Domains

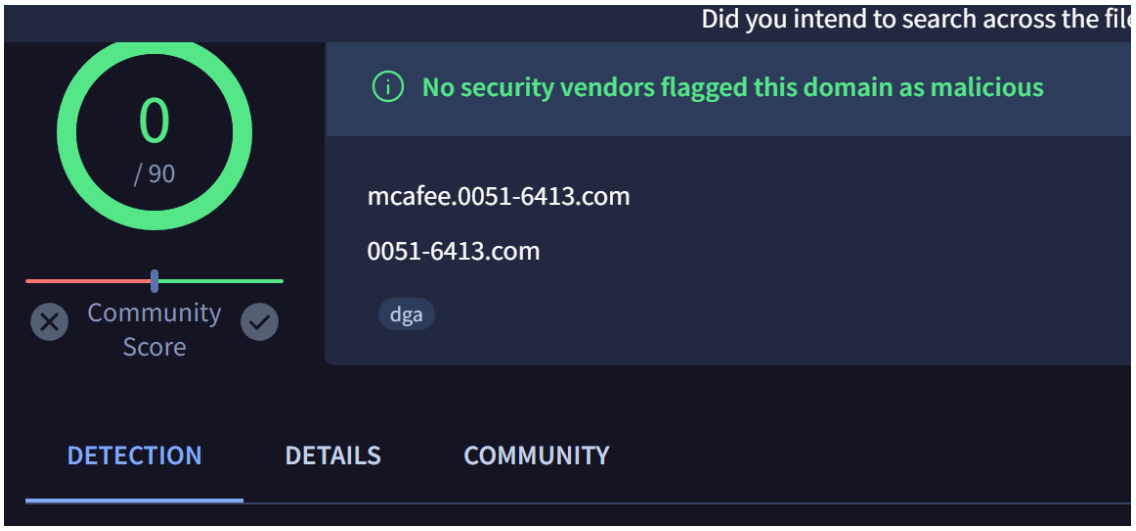
```
 mcafee.0041-3413[.]com
mcafee.0041-5413[.]com
mcafee.0051-4413[.]com
mcafee.0051-6413[.]com
mcafee.357-46[.]com
mcafee.486-31[.]com
mcafee.5541-23[.]com
mcafee.5814-1601[.]com
mcafee.5832-1414[.]com
mcafee.5832-3414[.]com
mcafee.654-87[.]com
mcafee.789-20[.]com
mcafee.798-13[.]com
```

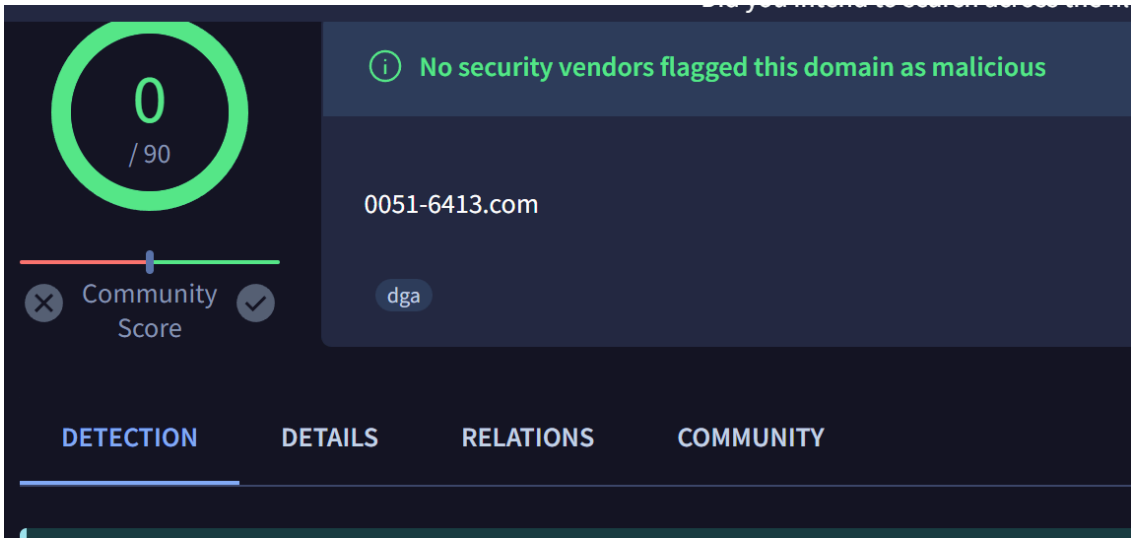
Virustotal Review

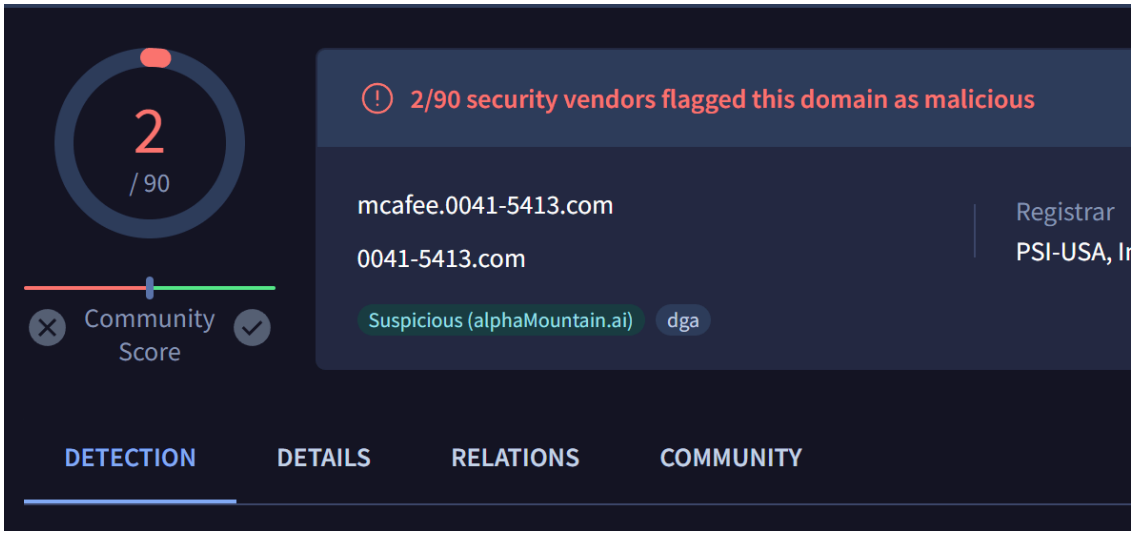


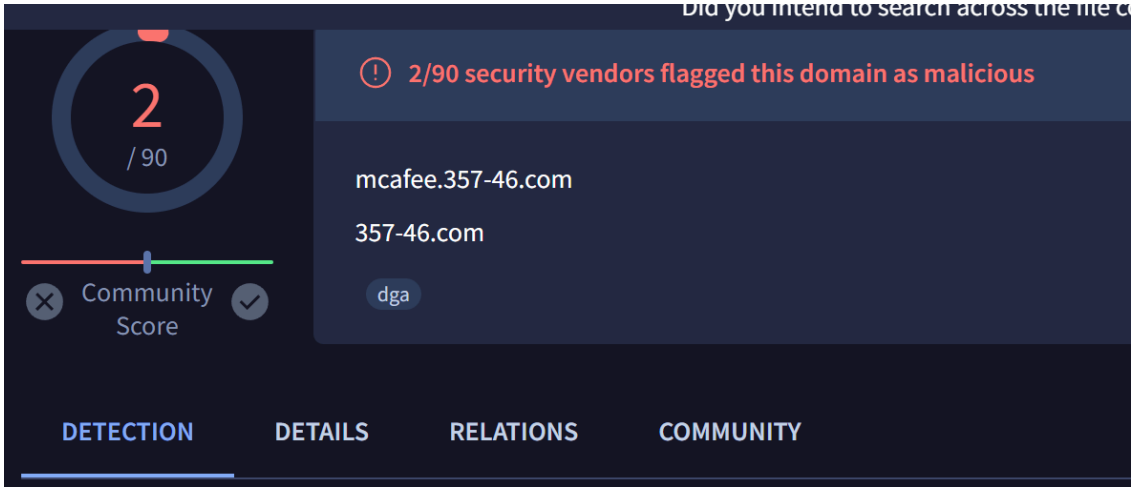


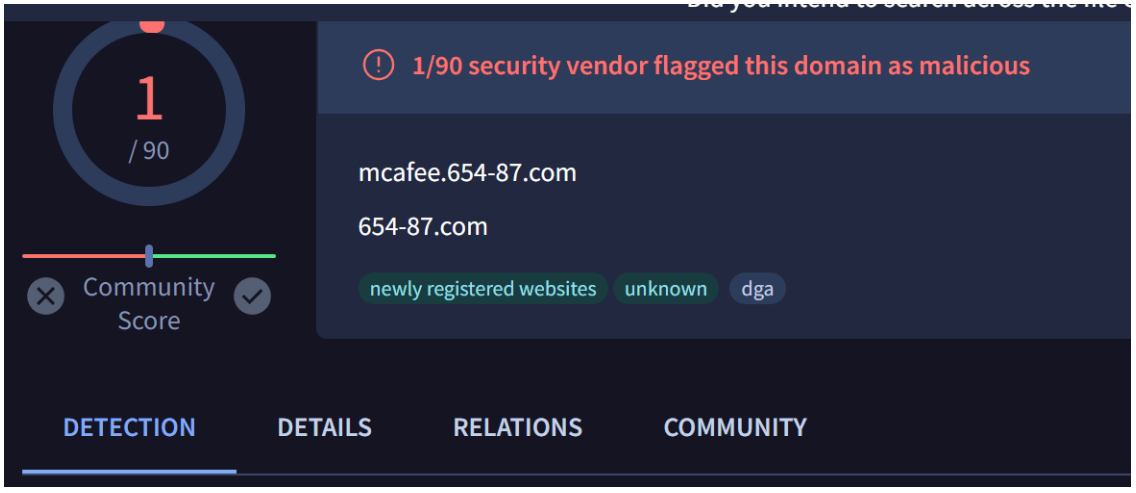

0
/ 90
Community Score
No security vendors flagged this domain as malicious
mcafee.0041-3413.com
0041-3413.com
dga
DETECTION
DETAILS
RELATIONS
COMMUNITY

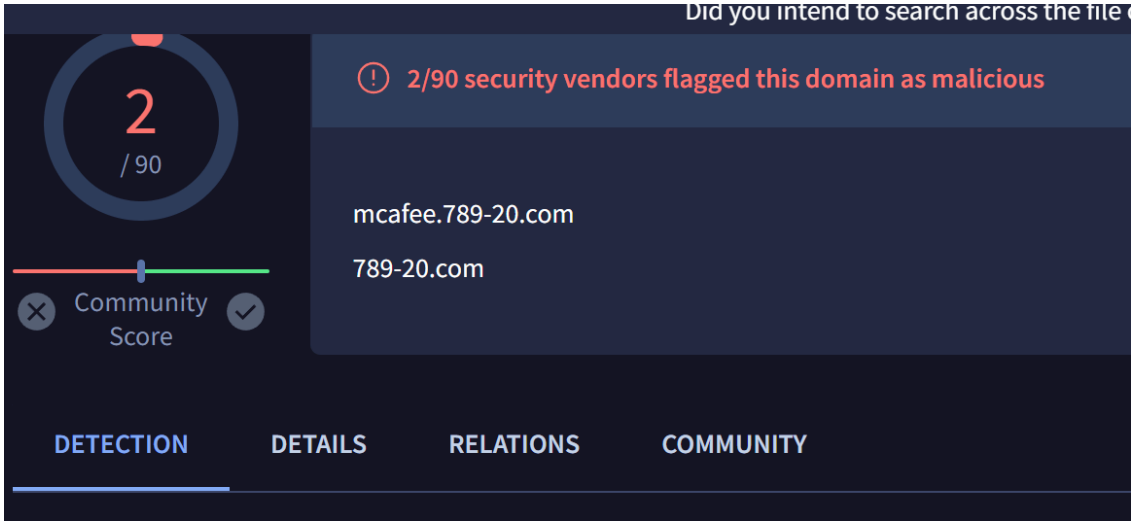

Did you intend to search across the fil
0
/ 90
Community Score
No security vendors flagged this domain as malicious
mcafee.0051-6413.com
0051-6413.com
dga
DETECTION
DETAILS
COMMUNITY


0
/ 90
Community Score
No security vendors flagged this domain as malicious
0051-6413.com
dga
DETECTION
DETAILS
RELATIONS
COMMUNITY


2
/ 90
Community Score
2/90 security vendors flagged this domain as malicious
mcafee.0041-5413.com
0041-5413.com
Suspicious (alphaMountain.ai)
dga
Registrar
PSI-USA, In
DETECTION
DETAILS
RELATIONS
COMMUNITY


2
/ 90
Community Score
2/90 security vendors flagged this domain as malicious
mcafee.357-46.com
357-46.com
dga
DETECTION
DETAILS
RELATIONS
COMMUNITY


1
/ 90
Community Score
1/90 security vendor flagged this domain as malicious
mcafee.654-87.com
654-87.com
newly registered websites
unknown
dga
DETECTION
DETAILS
RELATIONS
COMMUNITY



Sign up for Embee Research

Malware Analysis and Threat Intelligence Research

No spam. Unsubscribe anytime.

Source: https://embeeresearch.io/infrastructure-tracking-locating-vultur-domains-with-passive-dns/