Tracking Malware Infrastructure With Passive DNS and 302 Redirects

By Matthew

Published: 2024-04-01 · Archived: 2026-04-05 14:21:11 UTC

In this blog, we will identify 36 Latrodectus phishing domains through passive DNS analysis of a domain reported on Twitter/X.

The initial reported domain leverages 302 redirects to send users to a malicious or benign file. The URL in the 302 redirect is re-used across numerous domains; we can leverage this information to identify additional infrastructure.

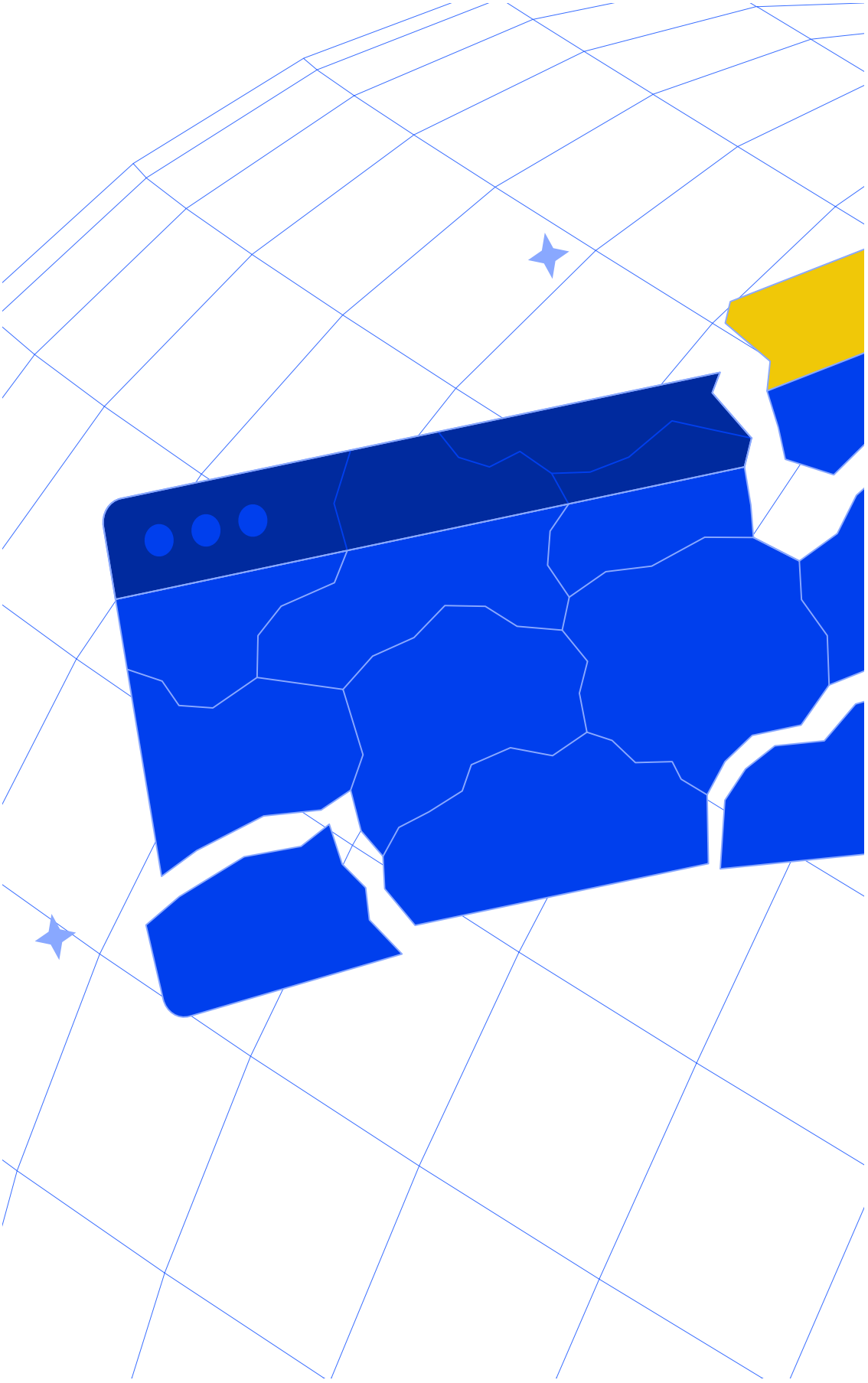
In summary, we will use the following indicators to identify the additional servers

- The same resolved IP address `193.106.174[.]218`
- The same usage of 302 redirects to the same URL on `documentcloud[.]org`
- Previous usage of 302 redirects to `harvardlawreview[.]org`

The primary tooling we will be leveraging is 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



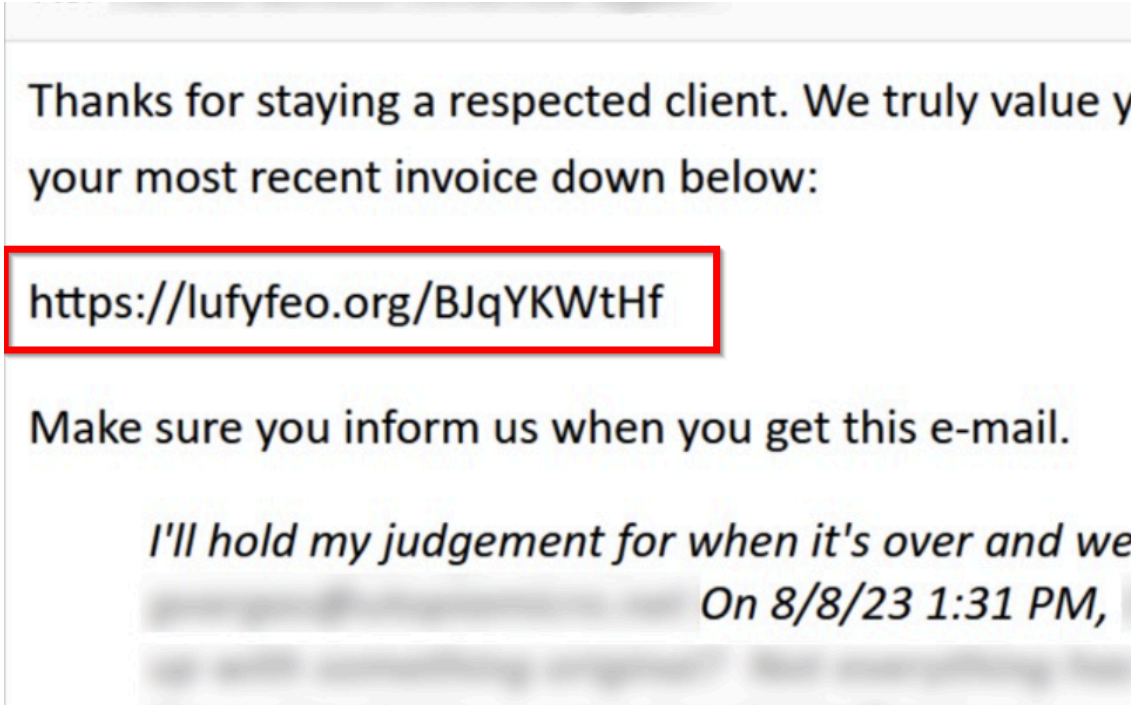
Initial Intelligence

The initial intelligence in this blog is from a tweet posted by @Unit42_intel.

The tweet details a Latrodectus infection leveraging phishing links to redirect victims to a javascript file, which ultimately loads LummaStealer Malware.

> 2024-03-07 (Thursday): #Latrodectus infection led to #LummaStealer. List of indicators available at https://t.co/8hYsKijuqX#Unit42ThreatIntel #TimelyThreatIntel #Wireshark #InfectionAnalysis #MaaS pic.twitter.com/ncEhMmjB72
>
> — Unit 42 (@Unit42_Intel) March 8, 2024

Within the original tweet, there is a screenshot of a phishing link contained in an email. This link contains the domain `lufyfeo[.]org`, which will form the basis and starting point of our analysis today.

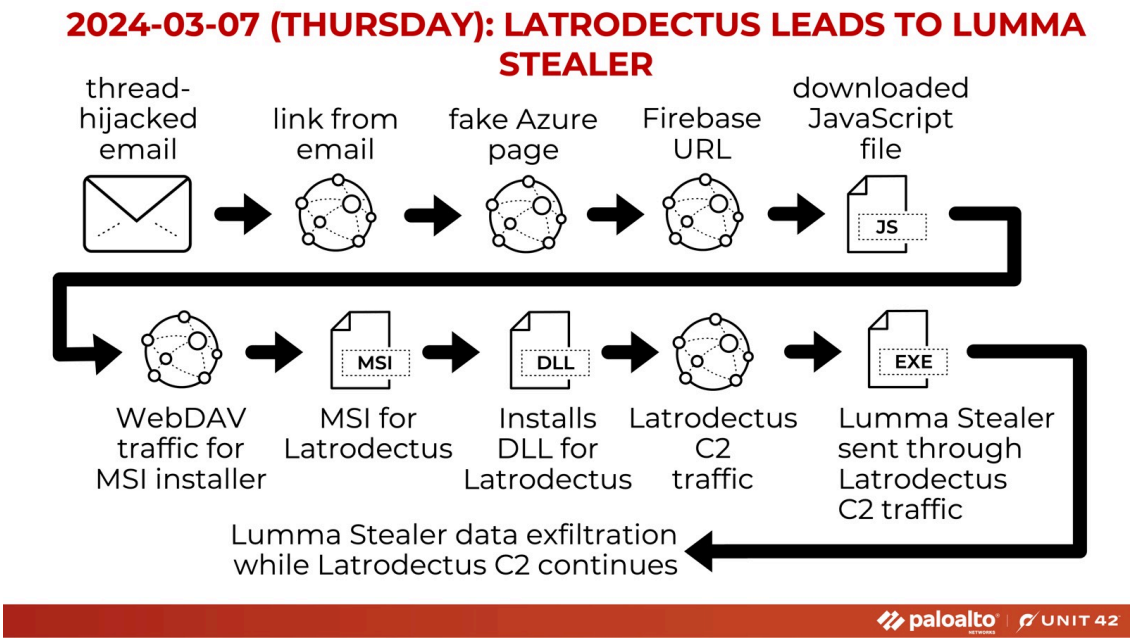


Our goal is to analyse this domain to identify patterns or indicators that can identify additional domains and IOCs.

Initial Notes

Based on information contained in the initial post, the `lufyfeo[.]org` domain is likely leveraging redirects to send a victim to alternate "fake" pages.

This information will form an important step in our next analysis, as we will leverage patterns in the 302 redirects to identify additional domains.



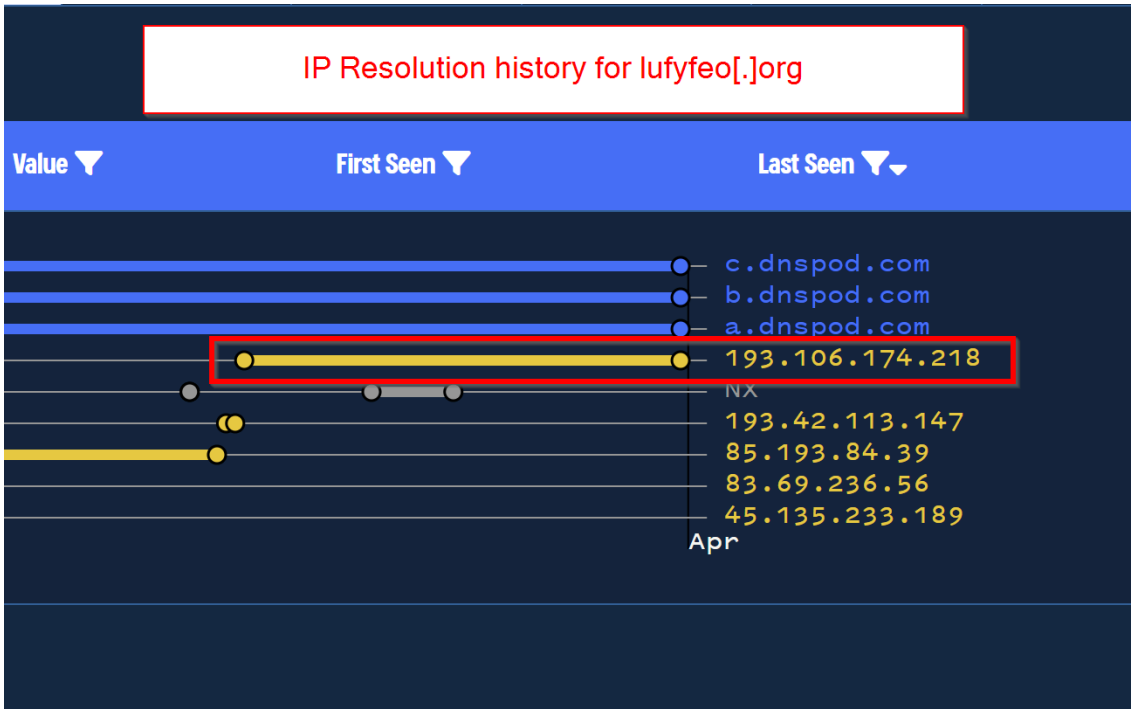
Initial Analysis With Passive DNS

Our initial analysis can begin by searching the `lufyfeo[.]org` domain using a passive DNS tool such as Validin.

This will reveal detailed history about resolved IP addresses have been in use by the domain.

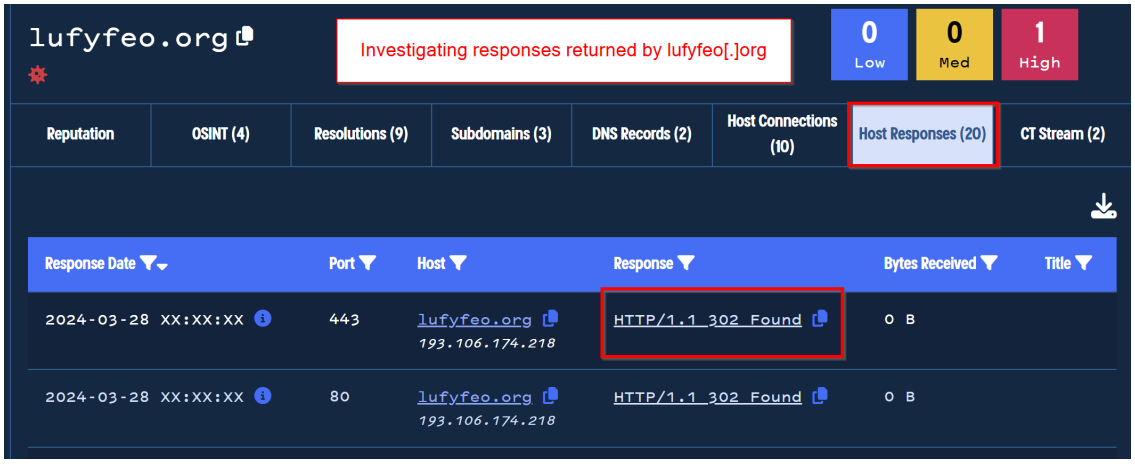
In the below screenshot, we can see that the most recent IP resolution was `193.106.174[.]218`

This IP address will form our first pivot point.



After determining the most recent IP address, we can also review the most recent host responses for the `lufyfeo[.]org` domain.

This reveals the presence of multiple 302 redirects, which are likely redirecting the user to the next malicious page.

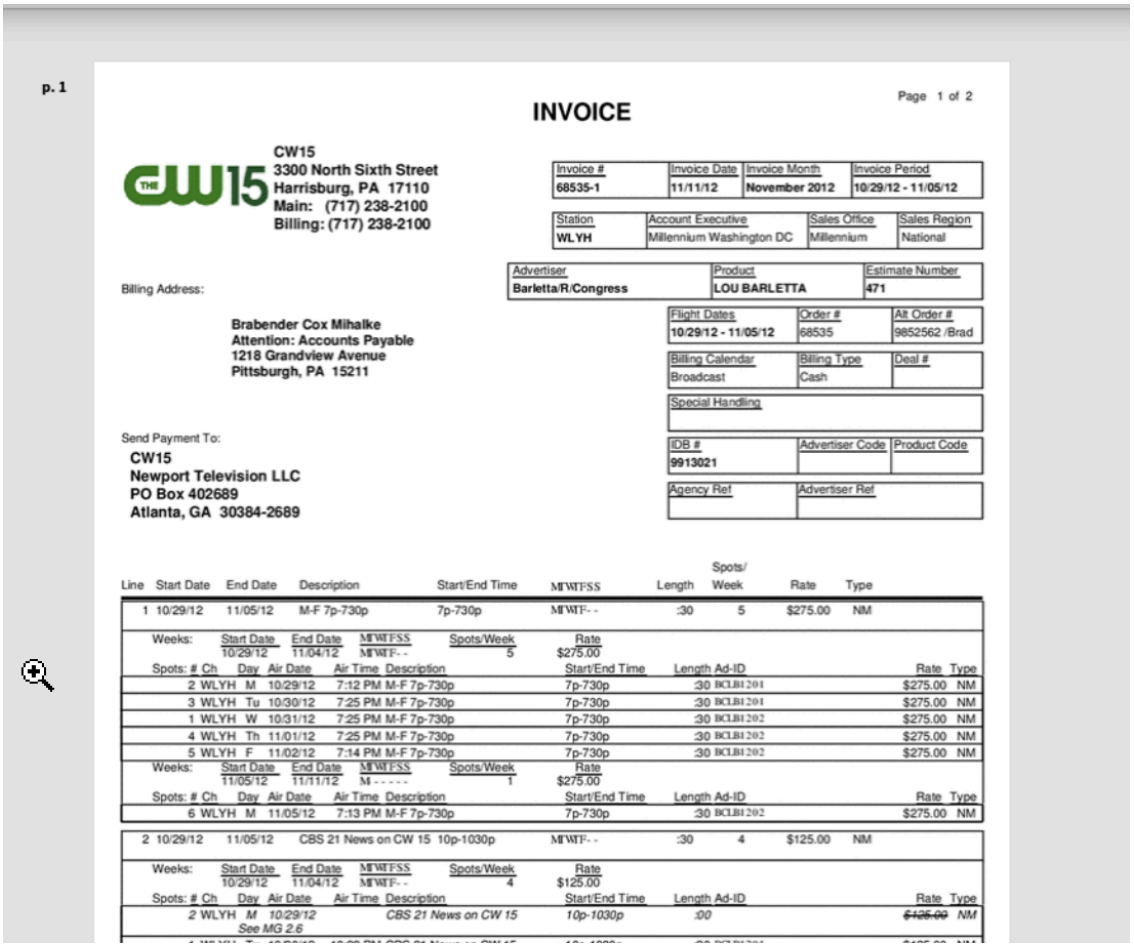


By viewing additional information about the 302 redirect, we can see that the redirect location is a PDF file hosted on `documentcloud[.]org`

By researching the `documentcloud[.]org` domain, this appears to be a legitimate site used for hosting pdf files.

Investigating this exact PDF link on urlscanAfter investigating this exact PDF link on urlscan, I found that it appears to be a relatively benign PDF file.

I did not confirm 100%, but I believe that this is a non-malicious PDF returned if the user has not requested the exact URL provided in the initial email.



p. 1

Page 1 of 2

INVOICE

CW15
3300 North Sixth Street
Harrisburg, PA 17110
Main: (717) 238-2100
Billing: (717) 238-2100

Invoice #	Invoice Date	Invoice Month	Invoice Period
68535-1	11/11/12	November 2012	10/29/12 - 11/05/12

Station	Account Executive	Sales Office	Sales Region
WLYH	Millennium Washington DC	Millennium	National

Advertiser	Product	Estimate Number
Barletta/R/Congress	LOU BARLETTA	471

Billing Address:

Brabender Cox Mihalke
Attention: Accounts Payable
1218 Grandview Avenue
Pittsburgh, PA 15211

Flight Dates	Order #	Alt Order #
10/29/12 - 11/05/12	68535	9852562 /Brad

Billing Calendar	Billing Type	Deal #
Broadcast	Cash	

Special Handling

IDB #	Advertiser Code	Product Code
9913021		

Agency Ref	Advertiser Ref

Send Payment To:
CW15
Newport Television LLC
PO Box 402689
Atlanta, GA 30384-2689

Line	Start Date	End Date	Description	Start/End Time	MTWTFSS	Length	Spots/ Week	Rate	Type
1	10/29/12	11/05/12	M-F 7p-730p	7p-730p	MTWTF- -	:30	5	$275.00	NM

Weeks:	Start Date	End Date	MTWTFSS	Spots/Week	Rate
	10/29/12	11/04/12	MTWTF- -	5	$275.00

Spots: #	Ch	Day	Air Date	Air Time	Description	Start/End Time	Length	Ad-ID	Rate	Type
2	WLYH	M	10/29/12	7:12 PM	M-F 7p-730p	7p-730p	:30	BCLBI201	$275.00	NM
3	WLYH	Tu	10/30/12	7:25 PM	M-F 7p-730p	7p-730p	:30	BCLBI201	$275.00	NM
1	WLYH	W	10/31/12	7:25 PM	M-F 7p-730p	7p-730p	:30	BCLBI202	$275.00	NM
4	WLYH	Th	11/01/12	7:25 PM	M-F 7p-730p	7p-730p	:30	BCLBI202	$275.00	NM
5	WLYH	F	11/02/12	7:14 PM	M-F 7p-730p	7p-730p	:30	BCLBI202	$275.00	NM

Weeks:	Start Date	End Date	MTWTFSS	Spots/Week	Rate
	11/05/12	11/11/12	M- - - - -	1	$275.00

Spots: #	Ch	Day	Air Date	Air Time	Description	Start/End Time	Length	Ad-ID	Rate	Type
6	WLYH	M	11/05/12	7:13 PM	M-F 7p-730p	7p-730p	:30	BCLBI202	$275.00	NM

2	10/29/12	11/05/12	CBS 21 News on CW 15 10p-1030p	MTWTF- -	:30	4	$125.00	NM

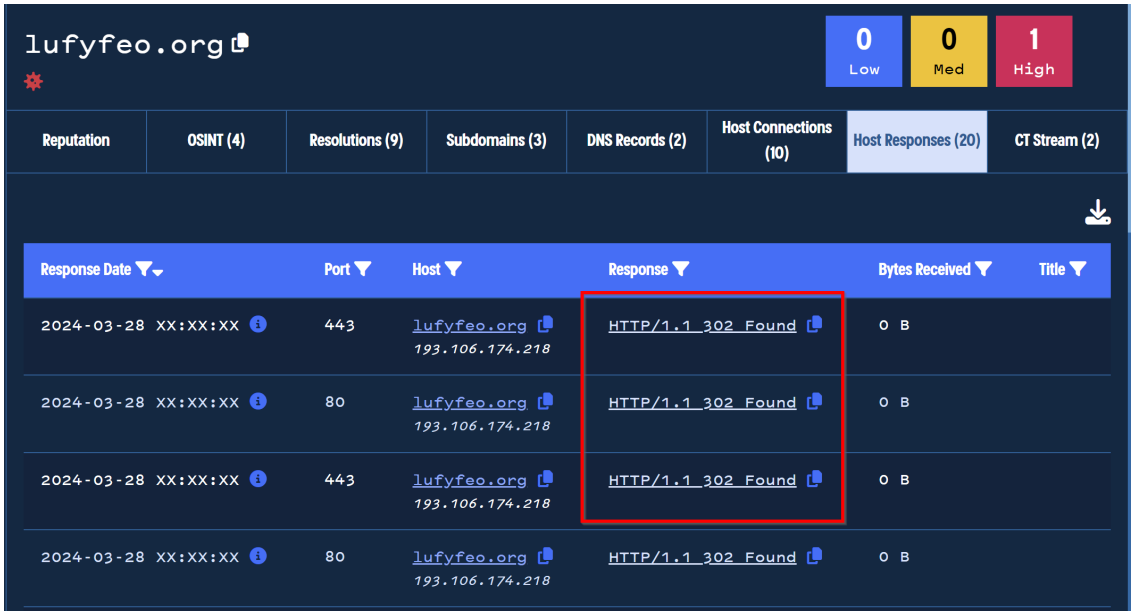
Weeks:	Start Date	End Date	MTWTFSS	Spots/Week	Rate
	10/29/12	11/04/12	MTWTF- -	4	$125.00

Spots: #	Ch	Day	Air Date	Air Time	Description	Start/End Time	Length	Ad-ID	Rate	Type
2	WLYH	M	10/29/12		CBS 21 News on CW 15	10p-1030p	:00		~~$125.00~~	NM
			See MG 2.6							

Leveraging Redirects as Pivot Points

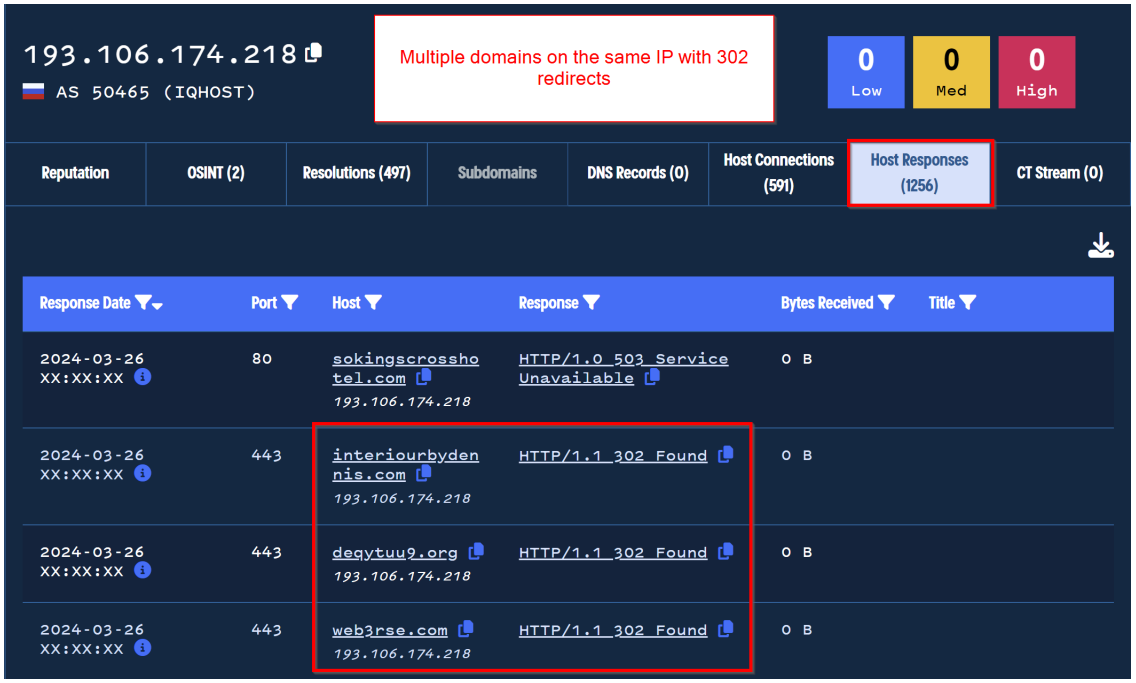
At this point, we have now identified the most recent IP address used by `lufyfeo[.]org`, and we have identified that the domain is leveraging 302 redirects to send the user to the next location.

Recall that the `lufyfeo[.]org` domain contains host responses with 302 redirects.



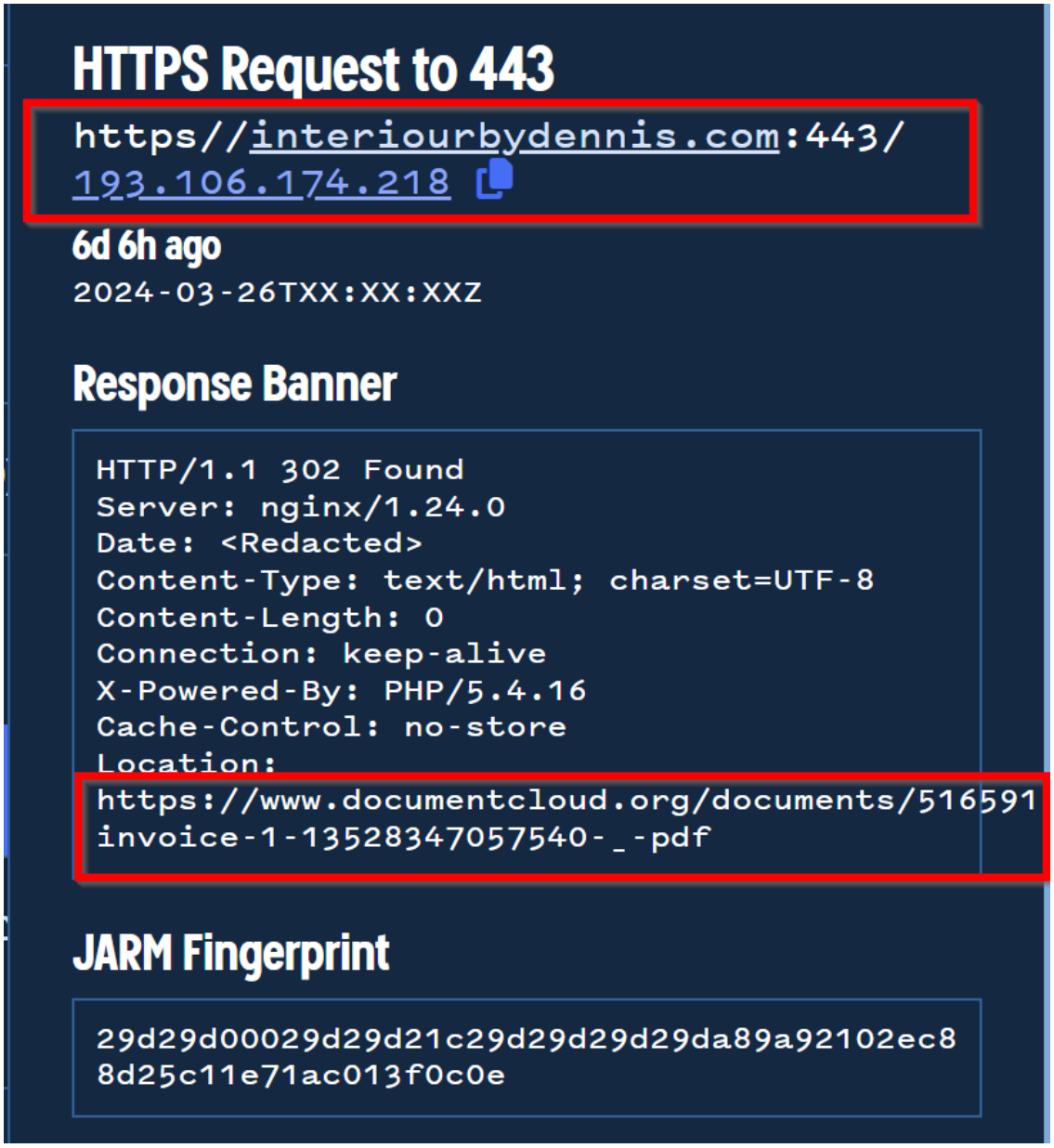
By expanding our search to the most recent resolved IP address for `lufyfeo[.]org`, we can expand this search to other domains hosted on the same server.

We can check this by searching for the most recent resolved IP `192.106.174[.]218` and checking the `Host Responses` tab for 302 redirects.



Reviewing the redirect details for `interiourbydennis[.]com`, we can see that the 302 redirects to the same location.

A very similar response can be observed for `deqytuu9[.]org` and `web3rse[.]org`



Of extremely interesting note is that the `deqytuu9[.]` domain resolves to a pdf file hosted on `harvardlawreview[.]org`

To my knowledge, this is a legitimate domain and legitimate file, but it is interesting to note that other sites hosting PDFs are being leveraged.

This will become more important later when we do additional pivoting.

Identifying All Current Domains

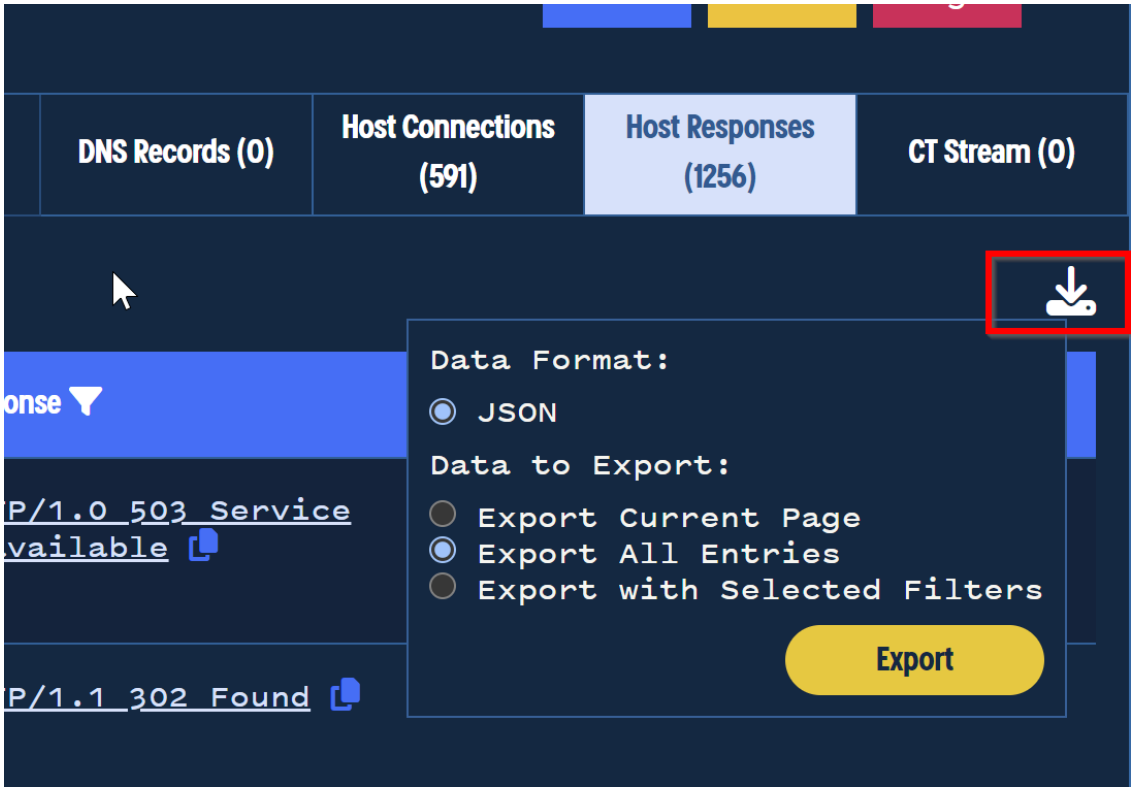
At this stage, we have identified an IP address `193.106.174[.]218` that is hosting both the original malicious domain `lufyfeo[.]org` as well as numerous other domains showing similar behaviour.

In total, there are 1256 host responses for the `193.106.174[.]218` address. Our next goal will be to enumerate all of these for indications of 302 redirects to URLs containing pdf references on `harvardlawreview[.]org` or `documentcloud[.]org`

Since the number of responses was so large, I utilised the JSON export feature of Validin to obtain the complete results of the search.

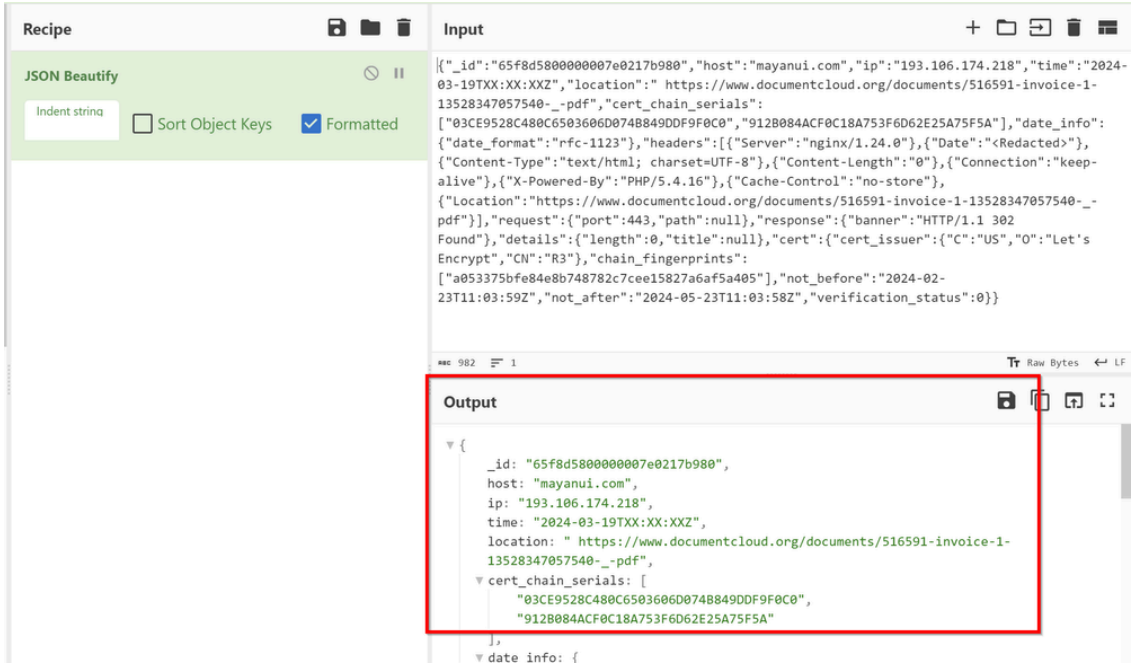
This allowed me to focus on information like the 302 redirect location.

We can start this by exporting all entries in the current response.



After exporting the entries, CyberChef can be leveraged to beautify the JSON output and determine which fields are of interest.

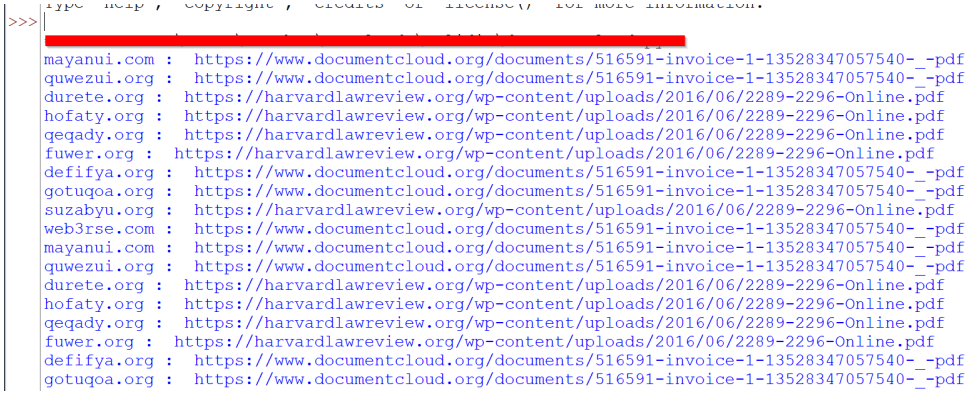
In this case, we want only the `host` and `location` fields within the JSON.



Enumerating JSON Output With Python

Since we only need to check the `location` and `host` fields, we can use a small Python script to enumerate all results in the JSON output for references to URLs with PDF references.

Running this script produces many results for redirects to the same location as the known malicious domain.



After deduplicating the results, we are left with 36 domains hosted on the same IP address and redirecting to the same `documentcloud[.]org` file, or the additional `harvardlawreview[.]org` file.

The complete list of these domains can be found below.

```
 mayanui[.]com
quwezui[.]org
durete[.]org
hofaty[.]org
qeqady[.]org
fuwer[.]org
defifya[.]org
gotuqoa[.]org
suzabyu[.]org
web3rse[.]com
interiourbydennis[.]com
```

```
sytukoe8[.]org
lufyfeo[.]org
boldenslawncare[.]com
qyjifia[.]org
vajosoo[.]org
sabehey[.]org
nevujo[.]org
lyzupoy[.]org
mypusau[.]org
zuwagie6[.]org
marypopkinz[.]com
simanay[.]org
cabobao3[.]org
ticava[.]org
zefos[.]org
fazadoe[.]org
luhuhu[.]org
cuxu[.]org
pubonao[.]org
xacygo[.]org
deqytuu9[.]org
gejyg[.]org
pucak[.]org
intellipowerinc[.]com
gejyg[.]org
```

Sign up for Embee Research

Malware Analysis, Detection Engineering and Threat Intelligence

No spam. Unsubscribe anytime.
