Investigating a Fake KDDI Smishing Campaign that abuses Duck DNS

By Lena

Published: 2023-06-23 · Archived: 2026-05-05 02:40:49 UTC

6 min read

Feb 19, 2023

Press enter or click to view image in full size

Recently in Japan, there has been an increase in Smishing attacks that abuse Duck DNS. In this blog post, I will be investigating one of these Duck DNS smishing attacks. The one analyzed here impersonates a mobile payment system.

Table of contents

The SMS message

The message says,

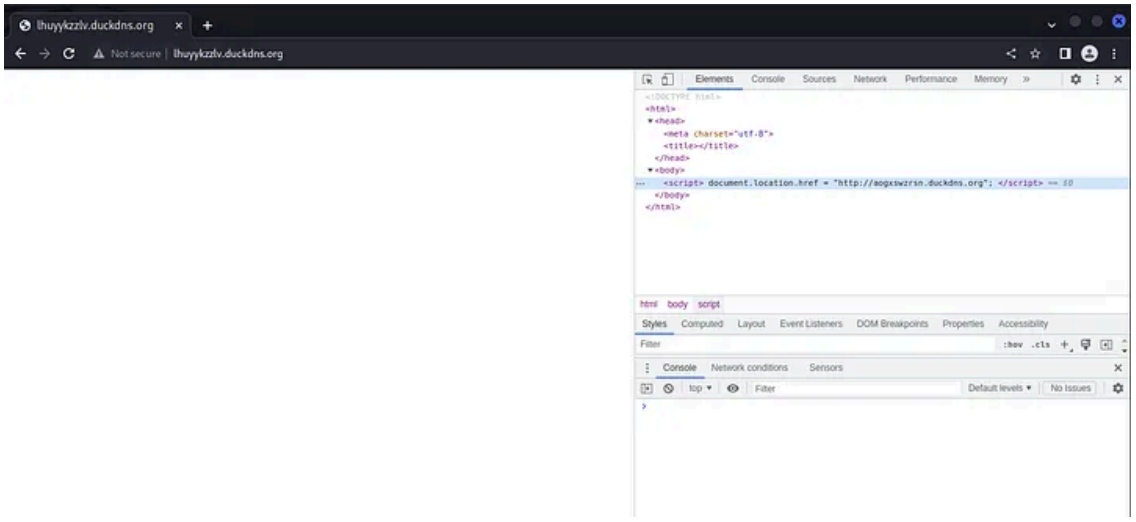
> 【利用停止予告】KDDI未払い料金お支払いのお願い。http://lhuyykzzlv[.]duckdns.org

Which translates to,

> [Suspension Notice] Please pay the unpaid KDDI fees. http://lhuyykzzlv[.]duckdns.org

Upon access, it leads to a blank page. Inspecting the element will show that it leads to another DuckDNS page.

Press enter or click to view image in full size

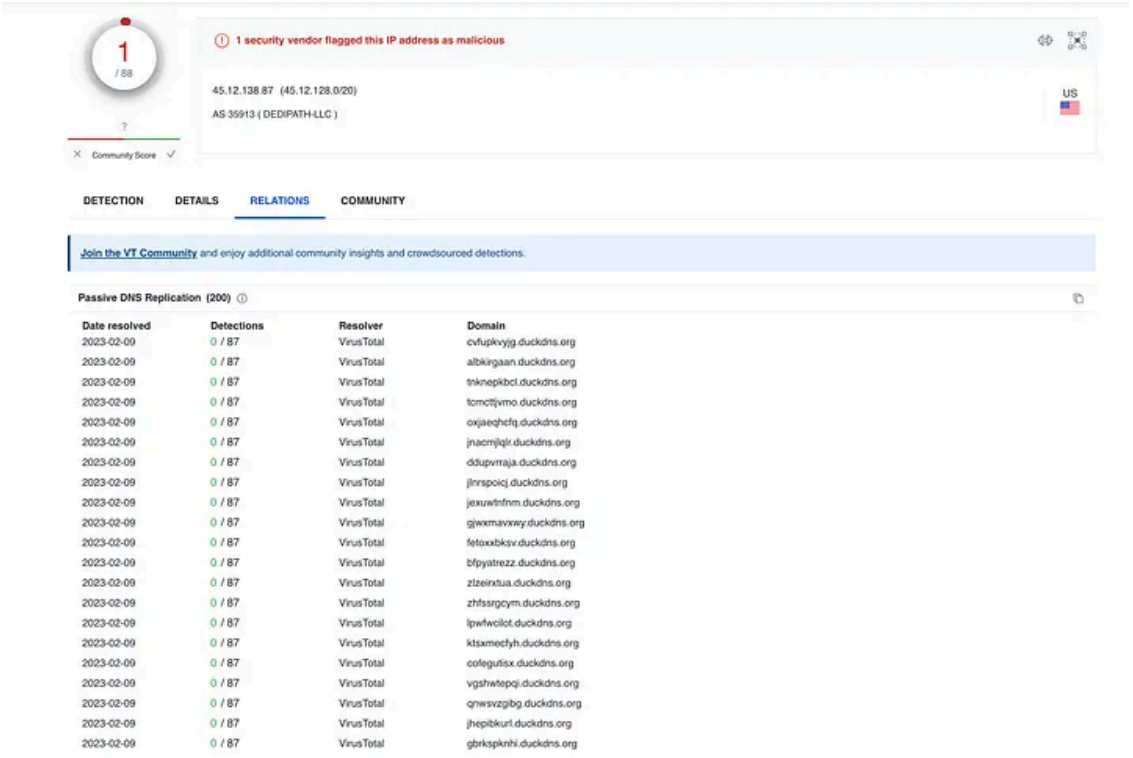


This page has an IP of 45.12.138[.]87.

Press enter or click to view image in full size

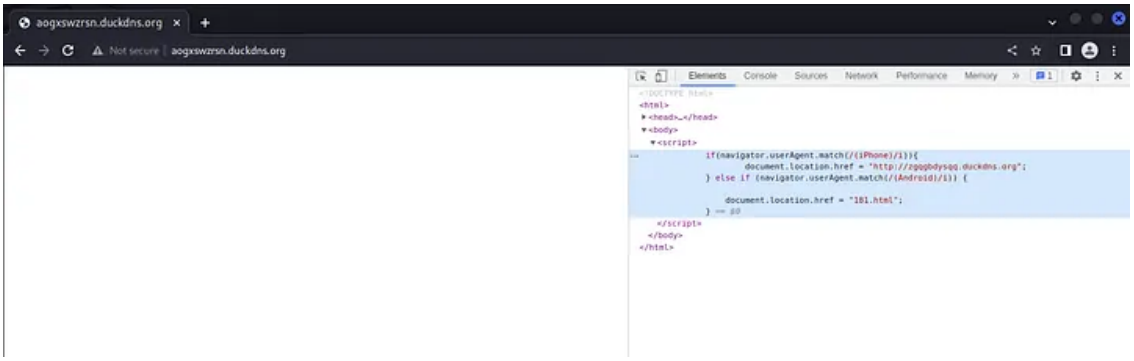
According to VirusTotal's Passive DNS Replication, it has many other Duck DNS domains associated with it.

Press enter or click to view image in full size



It then led me to another Duck DNS page. Inspecting the page showed that the next redirect will differ based on the User Agent. For an iPhone user agent, it will redirect to another Duck DNS page. For an Android user agent, it will redirect to `181.html` .

Press enter or click to view image in full size



This page also has an IP of 45.12.138[.]87.

Press enter or click to view image in full size

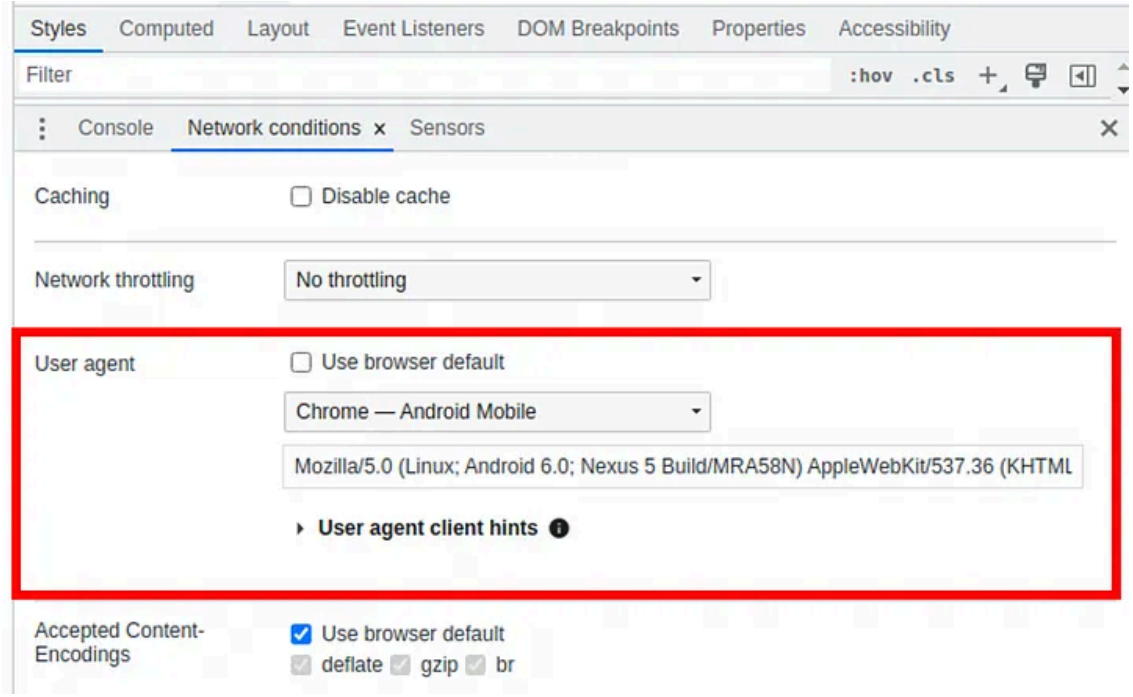
```
DNS     Standard query 0xd813 A aogxswzrsn.duckdns.org
DNS     Standard query response 0xd813 A aogxswzrsn.duckdns.org A 45.12.138.87
```

Android User-Agent

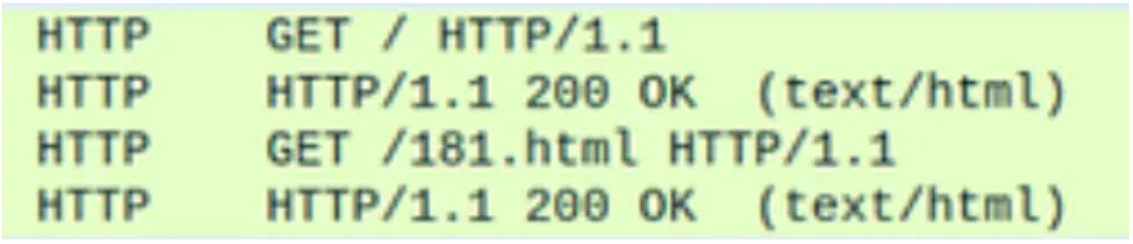
Under the “Network Conditions” tab in inspect element, I set the User-Agent to,

> Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Mobile Safari/537.36

Press enter or click to view image in full size

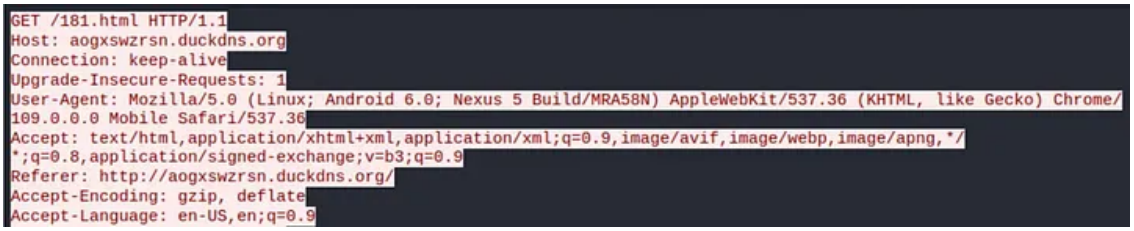


For an Android User-Agent, it will first lead to `/181.html`



The stream for the `181.html` GET request shows that it will redirect to another Duck DNS page.

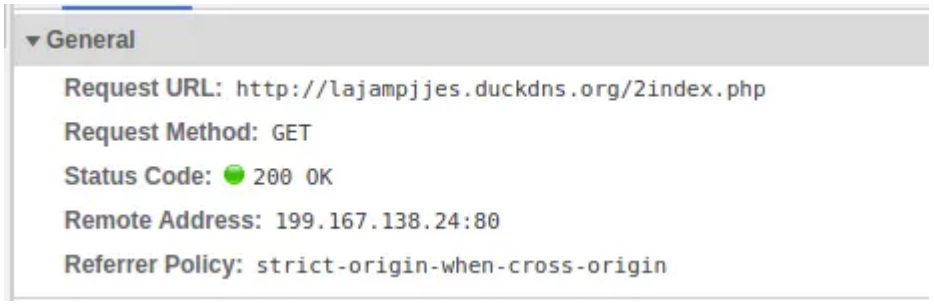
Press enter or click to view image in full size



Press enter or click to view image in full size

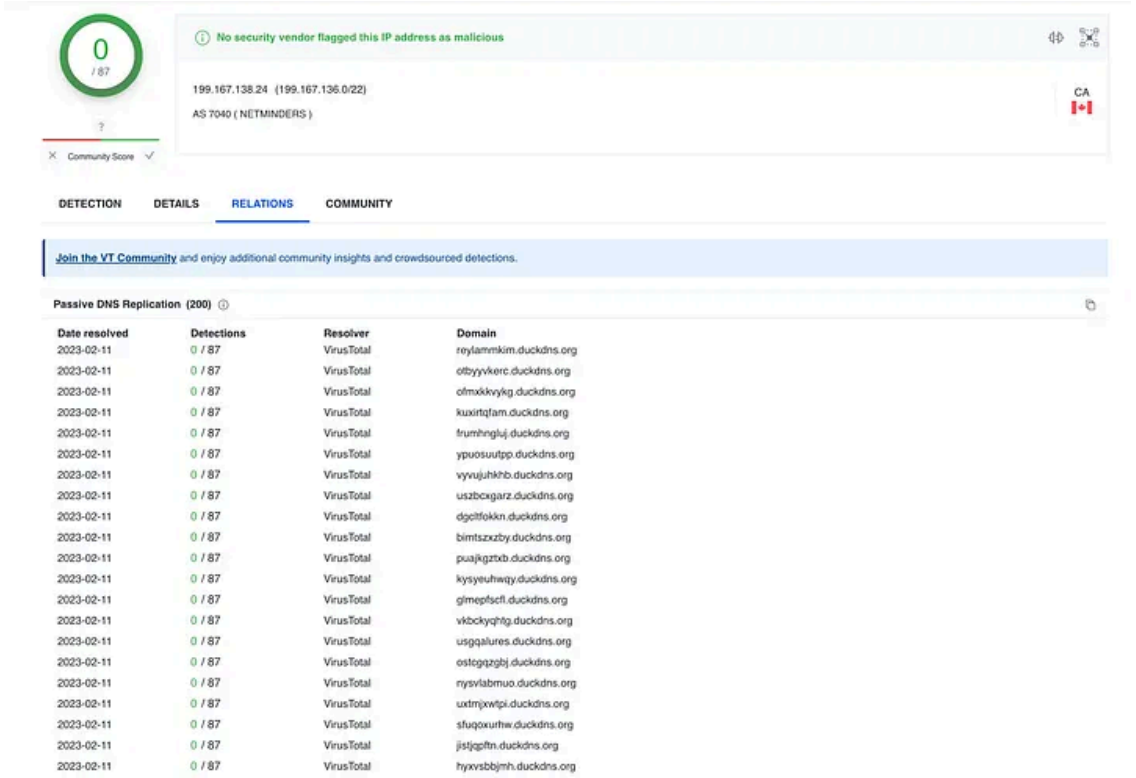
Press enter or click to view image in full size

The final Duck DNS page has an IP of 199.167.138[.]24.



The IP 199.167.138[.]24 also has many Duck DNS domains associated with it.

Press enter or click to view image in full size



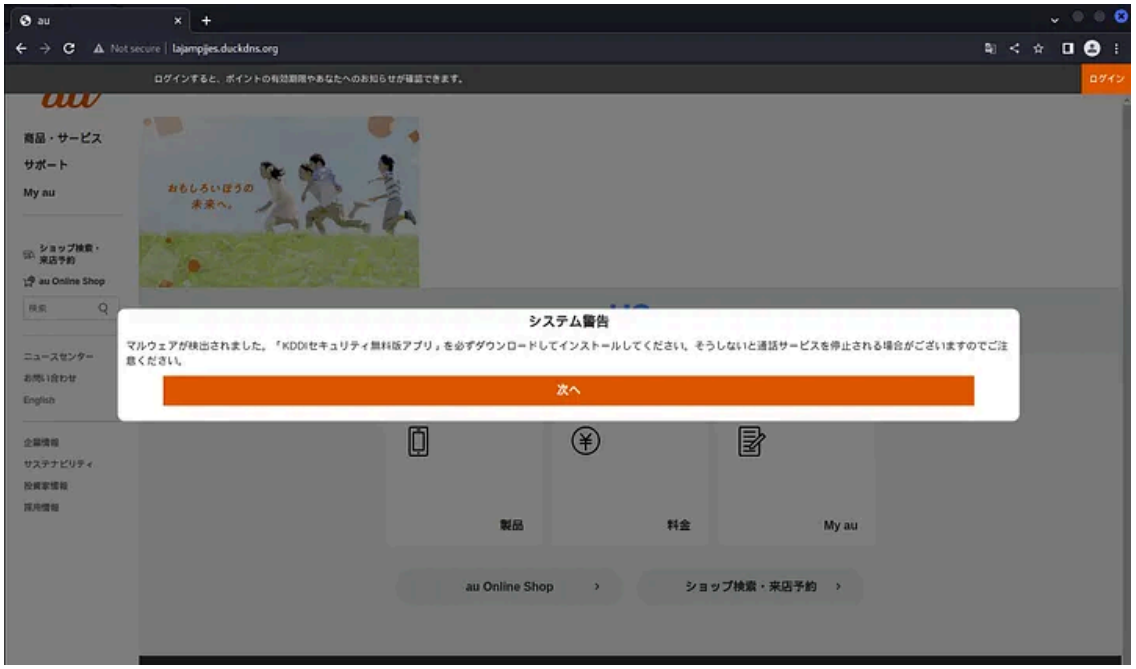
This final Duck DNS page shows a fake AU page with the following prompt,

> マルウェアが検出されました。「KDDIセキュリティ無料版アプリ」を必ずダウンロードしてインストールしてください。そうしないと通話サービスを停止される場合がございますのでご注意ください。

Which translates to,

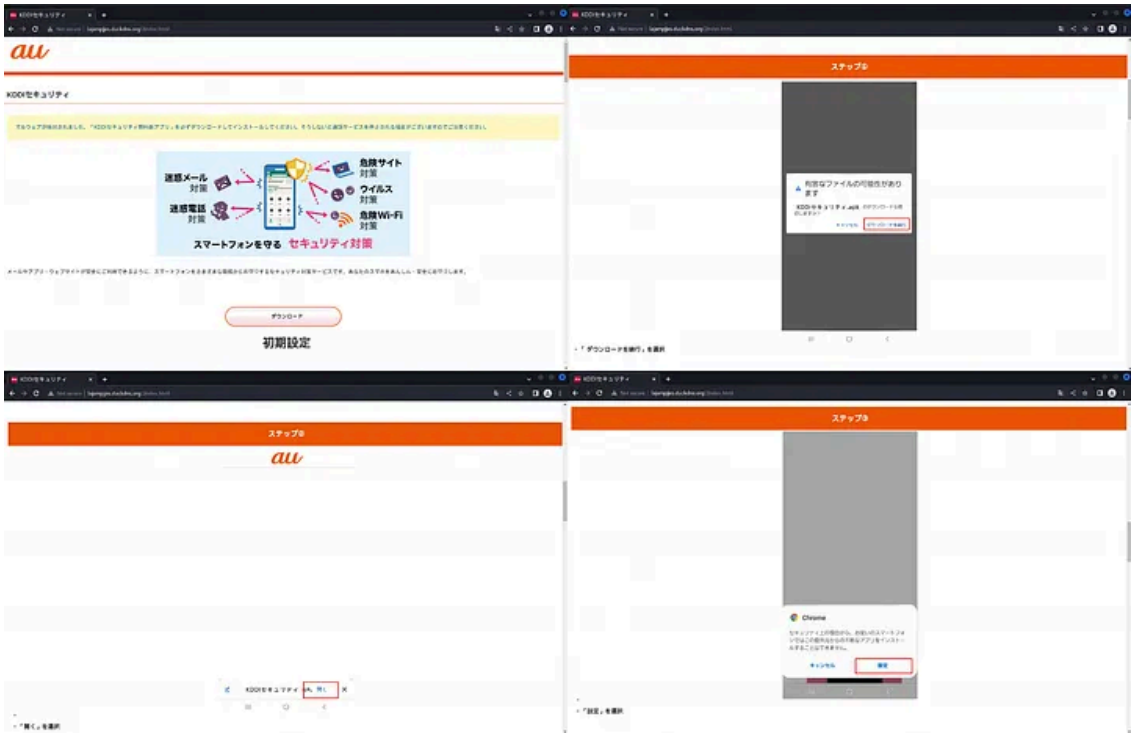
> Malware was detected on your device. Please be sure to download and install the “KDDI Security Free Edition App”. Please note that if you do not, the call service may be suspended.

Press enter or click to view image in full size

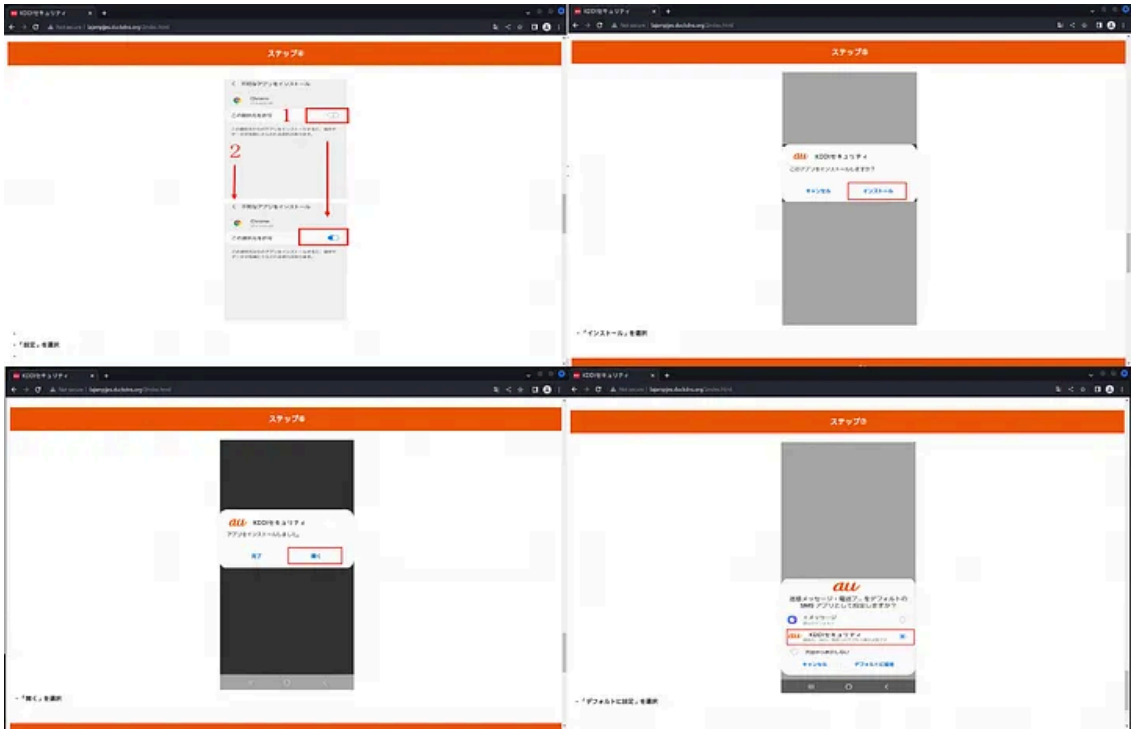


Clicking on 次へ (next) will lead to a download page. Scrolling through the page will show the install instructions.

Press enter or click to view image in full size



Press enter or click to view image in full size



Clicking on “Download” will download a file called `KDDI.apk`

Press enter or click to view image in full size

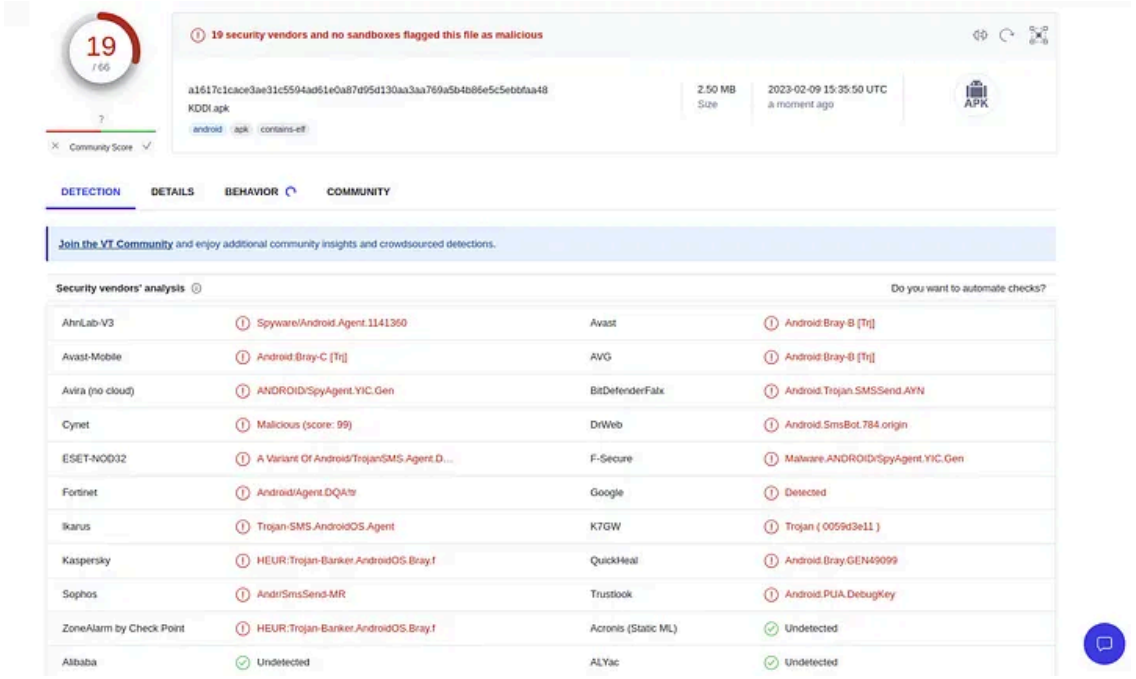
Get Lena’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

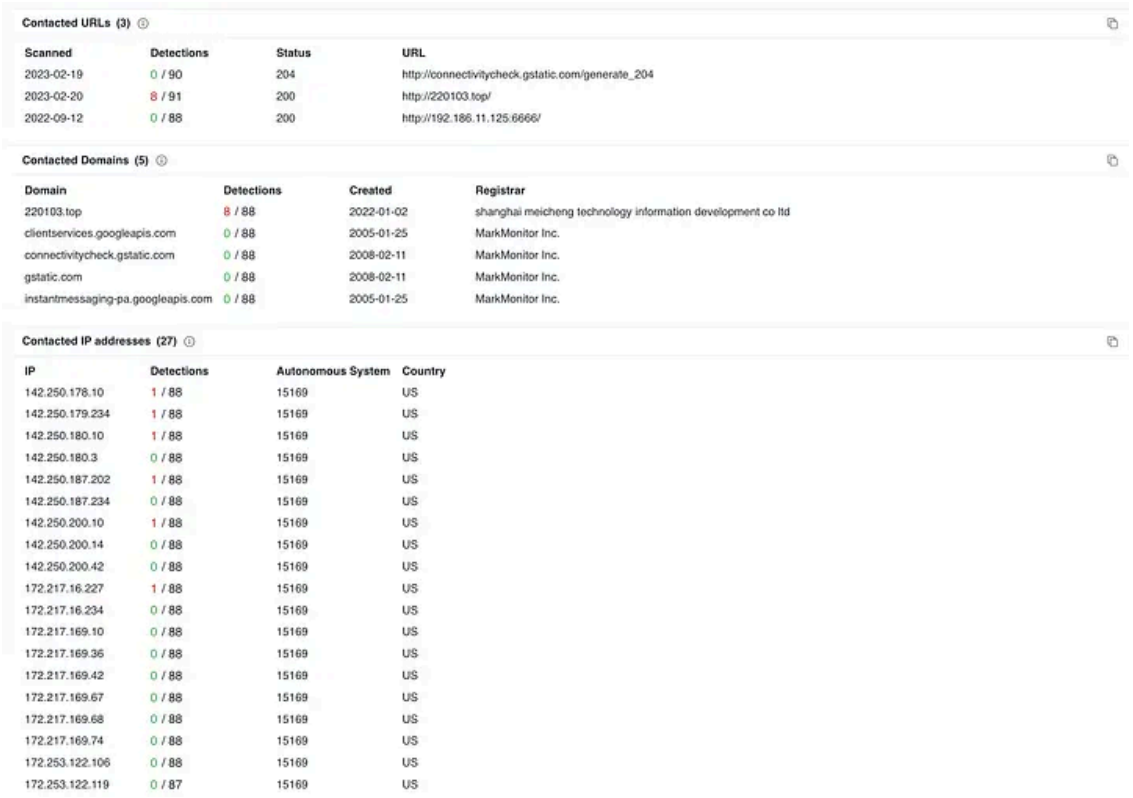
This `KDDI.apk` is flagged as [malicious by multiple vendors on VirusTotal.](#)

Press enter or click to view image in full size



This file contacts multiple URLs, domains and IP addresses.

Press enter or click to view image in full size



Contacted URLs (3)

Scanned	Detections	Status	URL
2023-02-19	0 / 90	204	http://connectivitycheck.gstatic.com/generate_204
2023-02-20	8 / 91	200	http://220103.top/
2022-09-12	0 / 88	200	http://192.186.11.125:6666/

Contacted Domains (5)

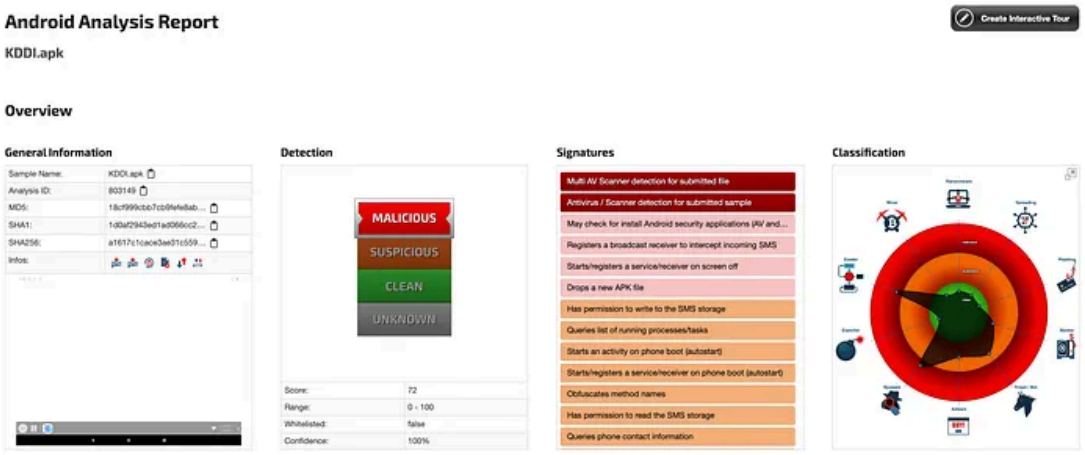
Domain	Detections	Created	Registrar
220103.top	8 / 88	2022-01-02	shanghai meicheng technology information development co ltd
clientservices.googleapis.com	0 / 88	2005-01-25	MarkMonitor Inc.
connectivitycheck.gstatic.com	0 / 88	2008-02-11	MarkMonitor Inc.
gstatic.com	0 / 88	2008-02-11	MarkMonitor Inc.
instantmessaging-pa.googleapis.com	0 / 88	2005-01-25	MarkMonitor Inc.

Contacted IP addresses (27)

IP	Detections	Autonomous System	Country
142.250.178.10	1 / 88	15169	US
142.250.179.234	1 / 88	15169	US
142.250.180.10	1 / 88	15169	US
142.250.180.3	0 / 88	15169	US
142.250.187.202	1 / 88	15169	US
142.250.187.234	0 / 88	15169	US
142.250.200.10	1 / 88	15169	US
142.250.200.14	0 / 88	15169	US
142.250.200.42	0 / 88	15169	US
172.217.16.227	1 / 88	15169	US
172.217.16.234	0 / 88	15169	US
172.217.169.10	0 / 88	15169	US
172.217.169.36	0 / 88	15169	US
172.217.169.42	0 / 88	15169	US
172.217.169.67	0 / 88	15169	US
172.217.169.68	0 / 88	15169	US
172.217.169.74	0 / 88	15169	US
172.253.122.106	0 / 88	15169	US
172.253.122.119	0 / 87	15169	US

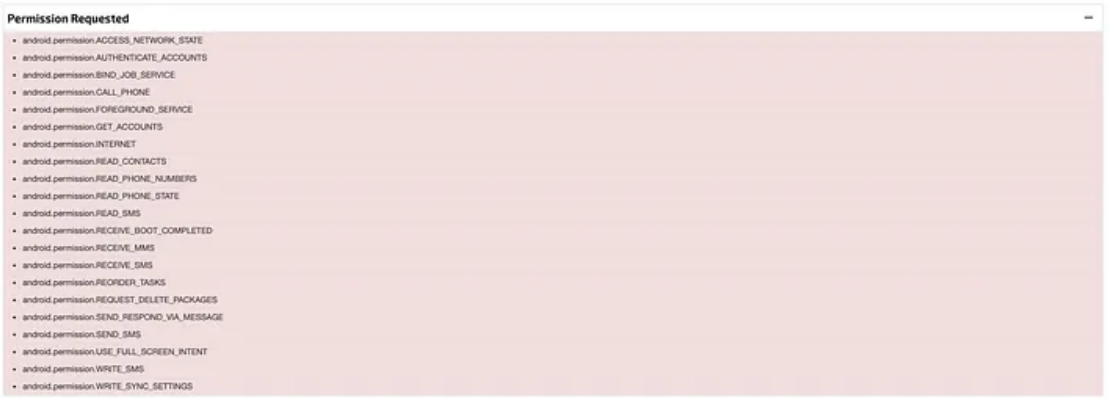
JoeSandbox detected `KDDI.apk` as malicious, and many suspicious behaviours can be seen.

Press enter or click to view image in full size



`KDDI.apk` makes various permission requests such as `android.permission.SEND_SMS`, `android.permission.CALL_PHONE`, `android.permission.WRITE_SMS`.

Press enter or click to view image in full size



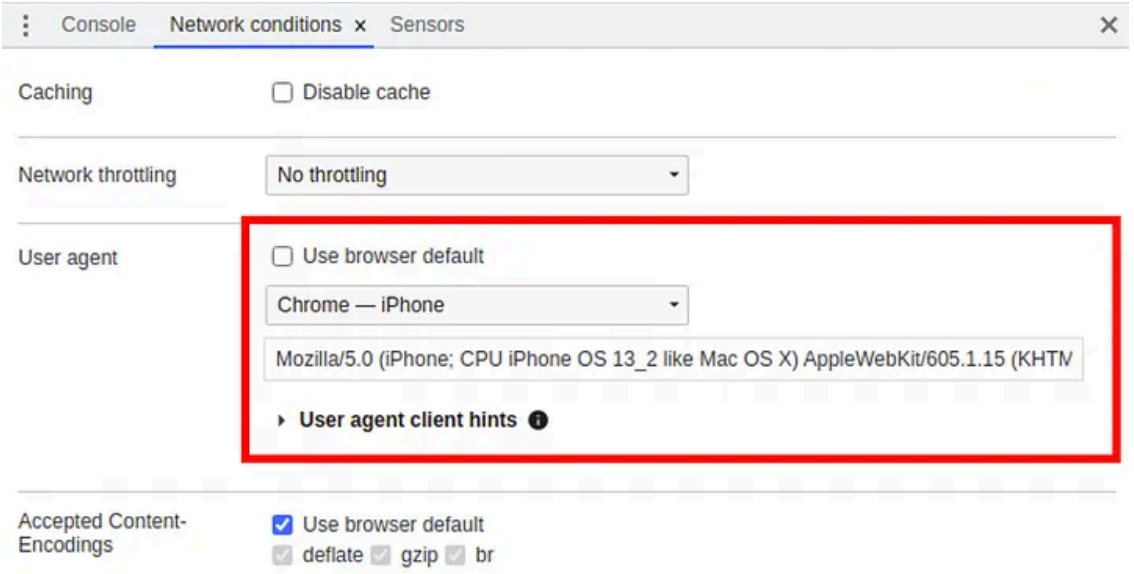
The full analysis on JoeSandbox can be found here,

iPhone User-Agent

Under the “Network Conditions” tab in inspect element, I set the User-Agent to,

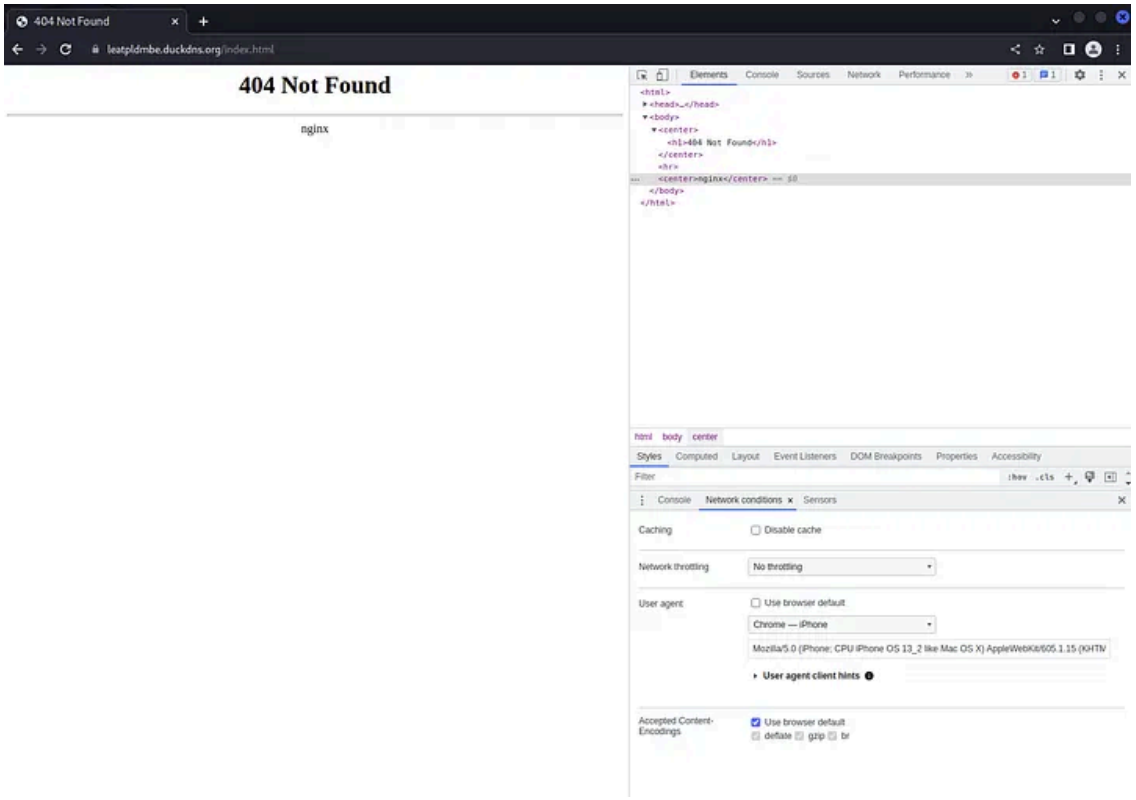
> Mozilla/5.0 (iPhone; CPU iPhone OS 13_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/109.0.0.0 Mobile/15E148 Safari/604.1

Press enter or click to view image in full size



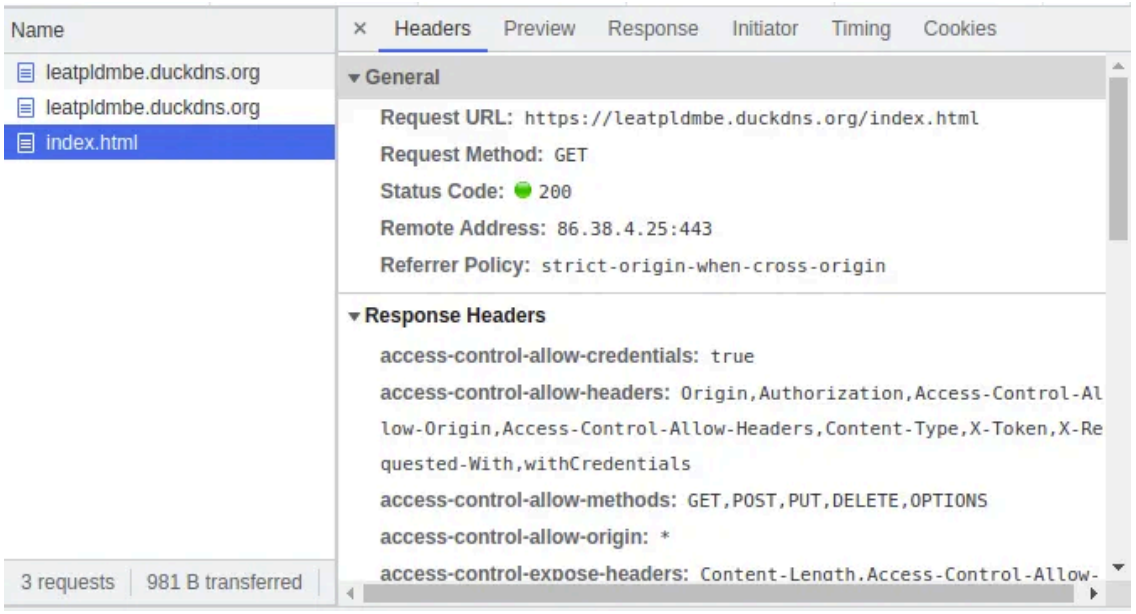
It leads to `index.html`, however, “404 Not Found” was displayed.

Press enter or click to view image in full size



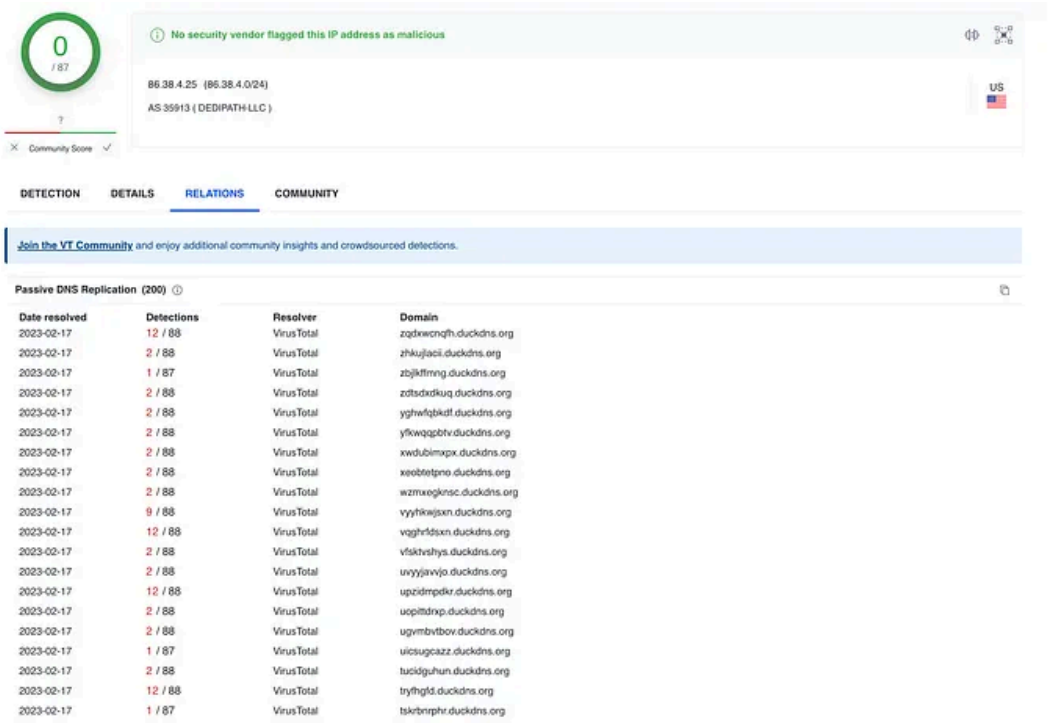
Inspecting the headers showed the following,

Press enter or click to view image in full size

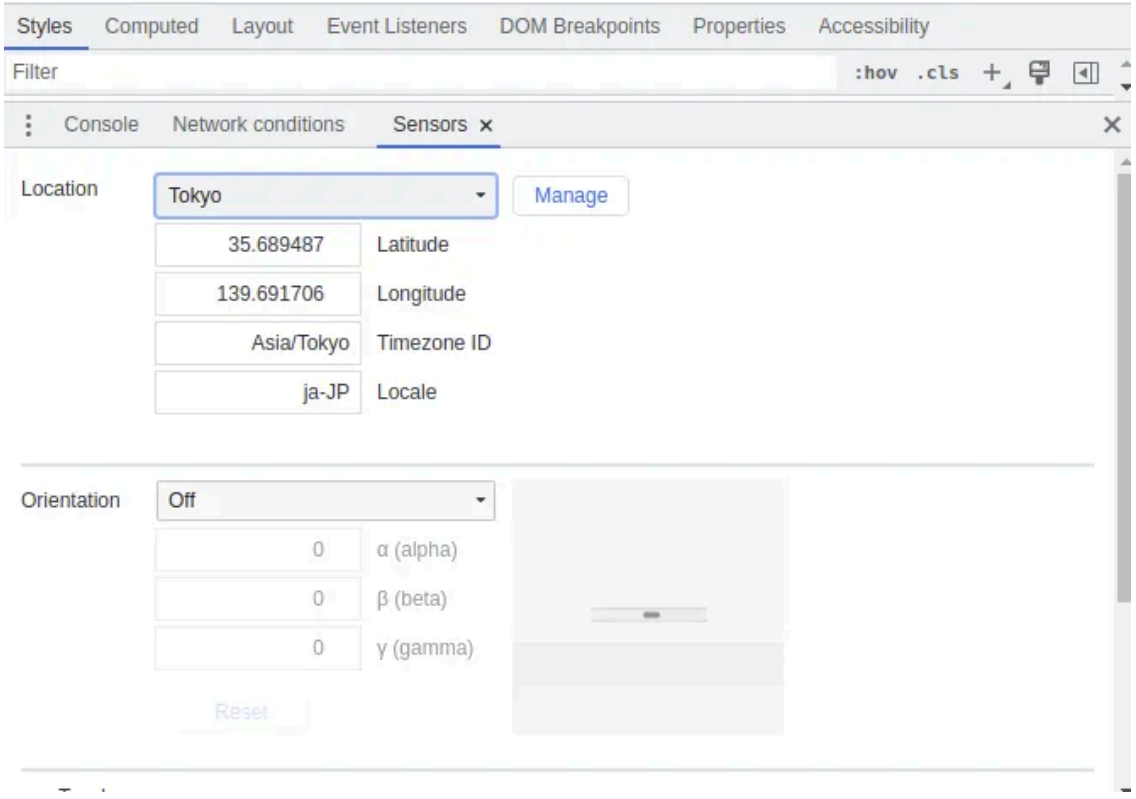


This page has an IP of 86.38.4[.]25, and has many other Duck DNS domains associated with it. A lot of them are flagged as malicious on VirusTotal.

Press enter or click to view image in full size

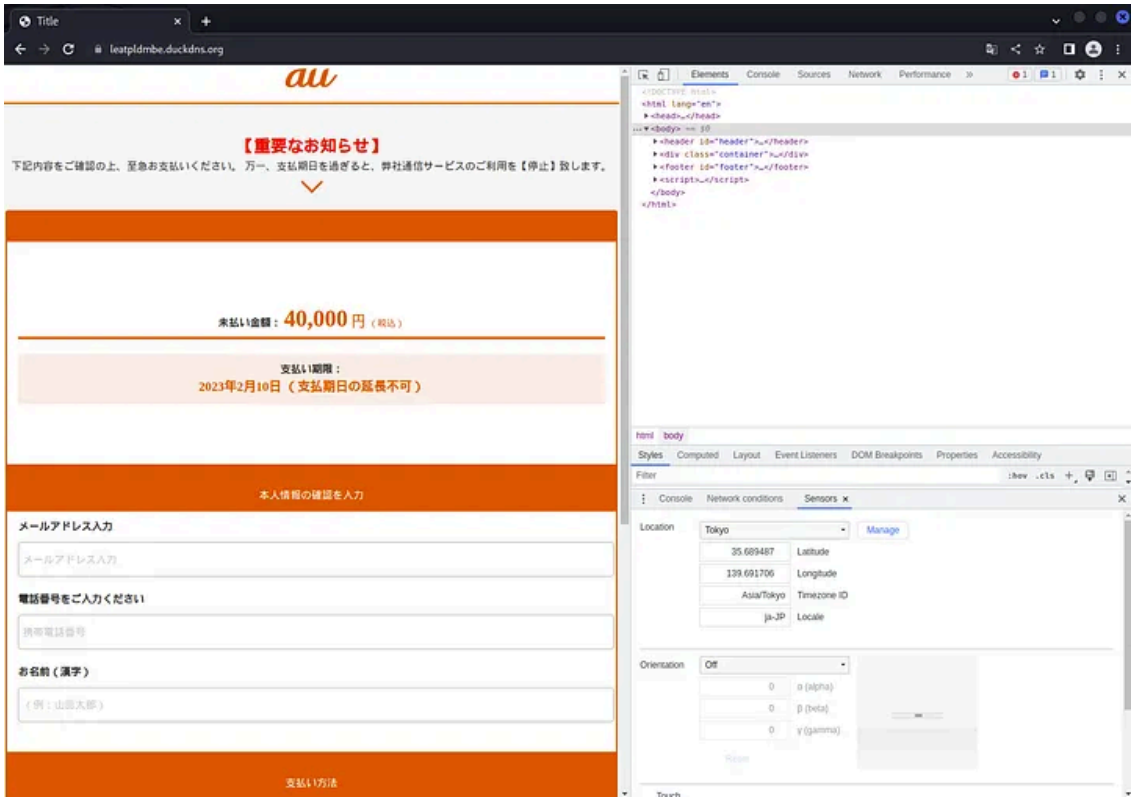


Since I could not access the site's contents, I went to the `Sensors` tab and set the location to `Tokyo` , with the Locale set to `ja-JP` .



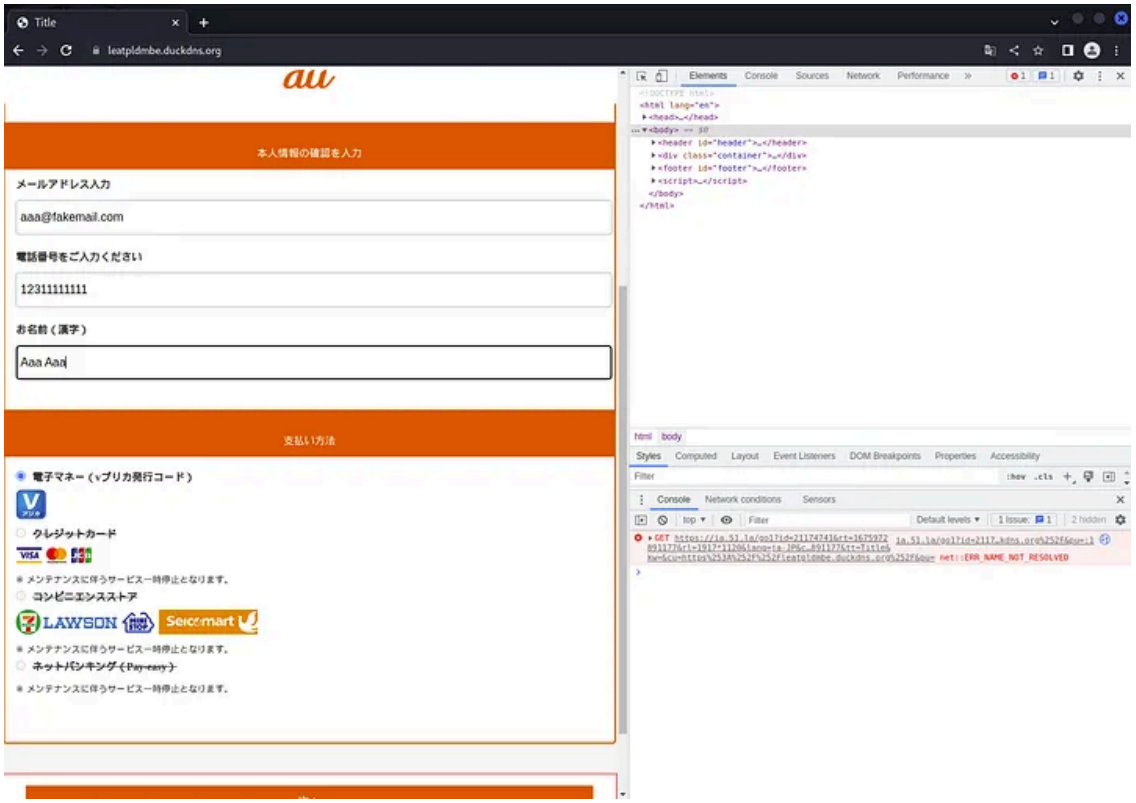
Reloading the page leads to a fake AU page that asks for the user's mail address, phone number, and name.

Press enter or click to view image in full size



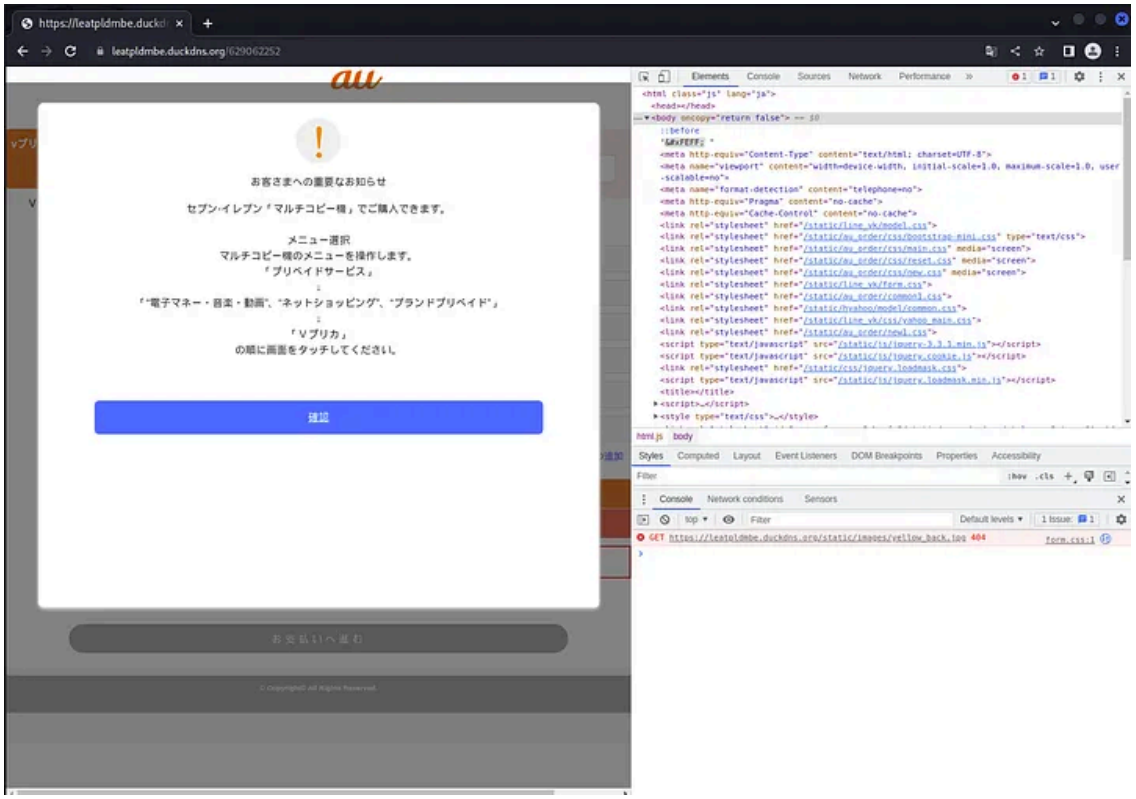
I entered some fake credentials and had to select a payment method. There seemed to be multiple payment options, but everything except 電子マネー (Electronic money) was crossed out.

Press enter or click to view image in full size



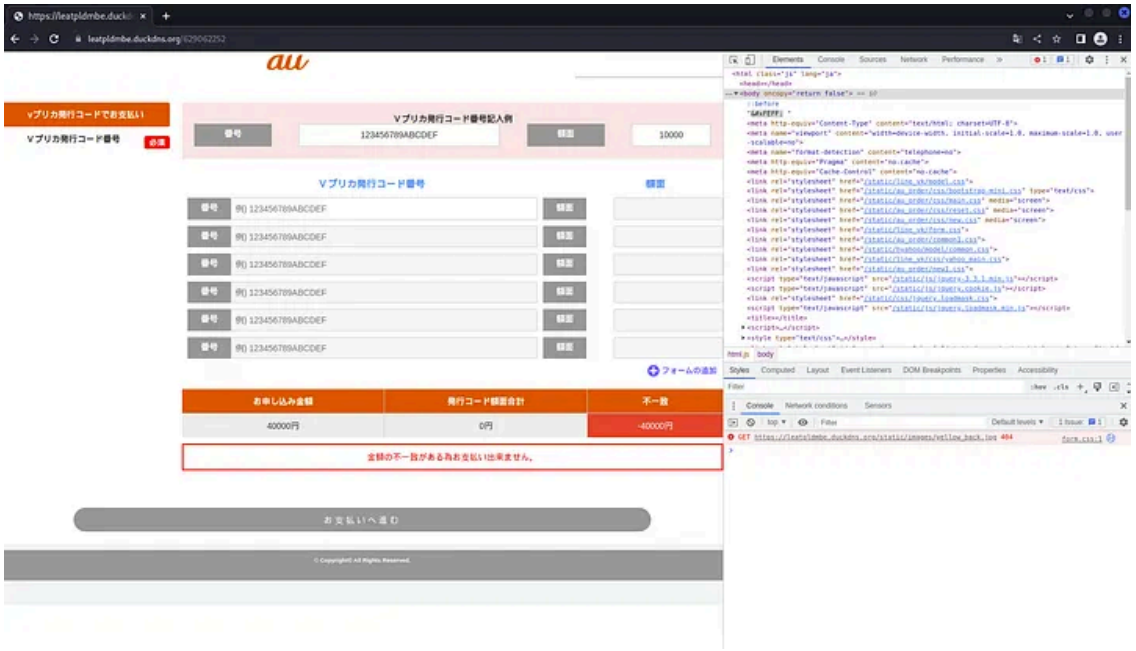
Submitting the credentials leads to a page that says the payment must be made using `Vプリカ` , which is a prepaid card.

Press enter or click to view image in full size



It then prompts the user to enter the `Vプリカ` (prepaid card) numbers.

Press enter or click to view image in full size

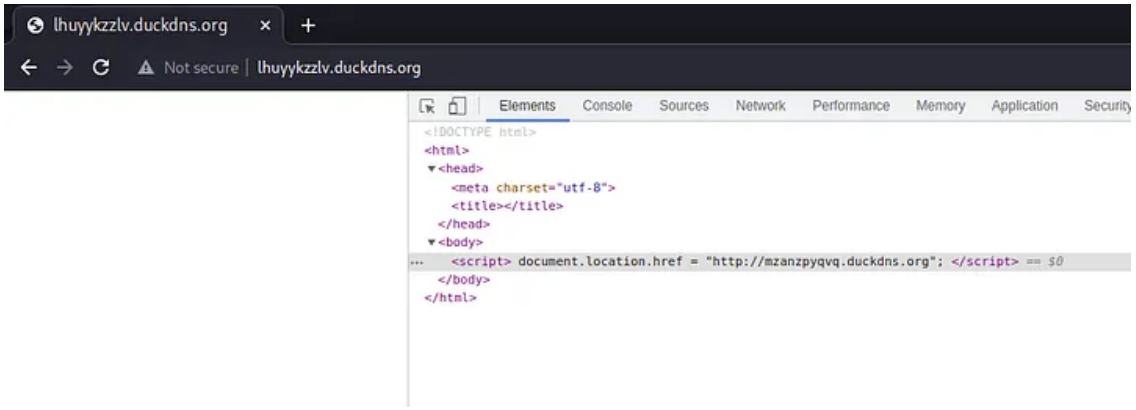


`Vプリカ` is a Visa prepaid card that can be used online. More details on `Vプリカ` can be found below,

Duck DNS behaviour

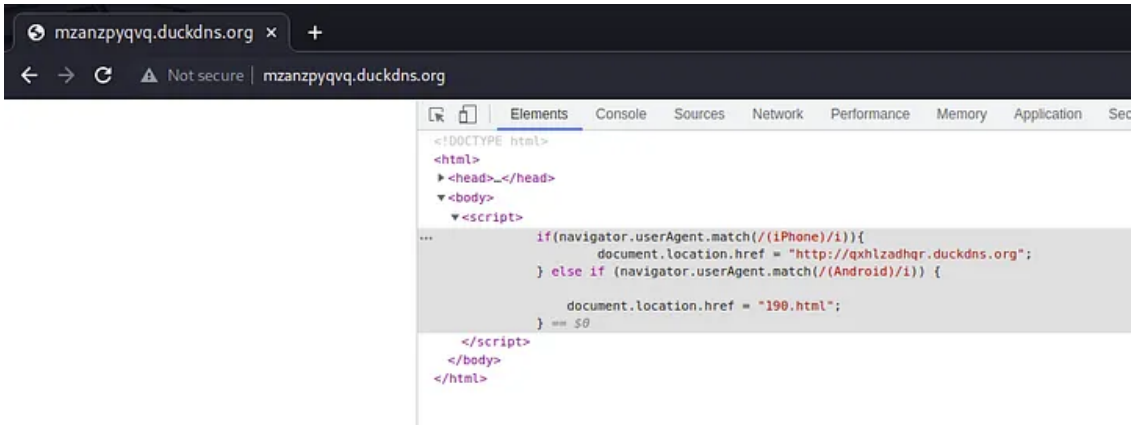
The redirect link changes very frequently. The first link is lhuyykzzlv.duckdns[.]org in this case, but it redirects to a different Duck DNS link every few mins-hours.

Press enter or click to view image in full size



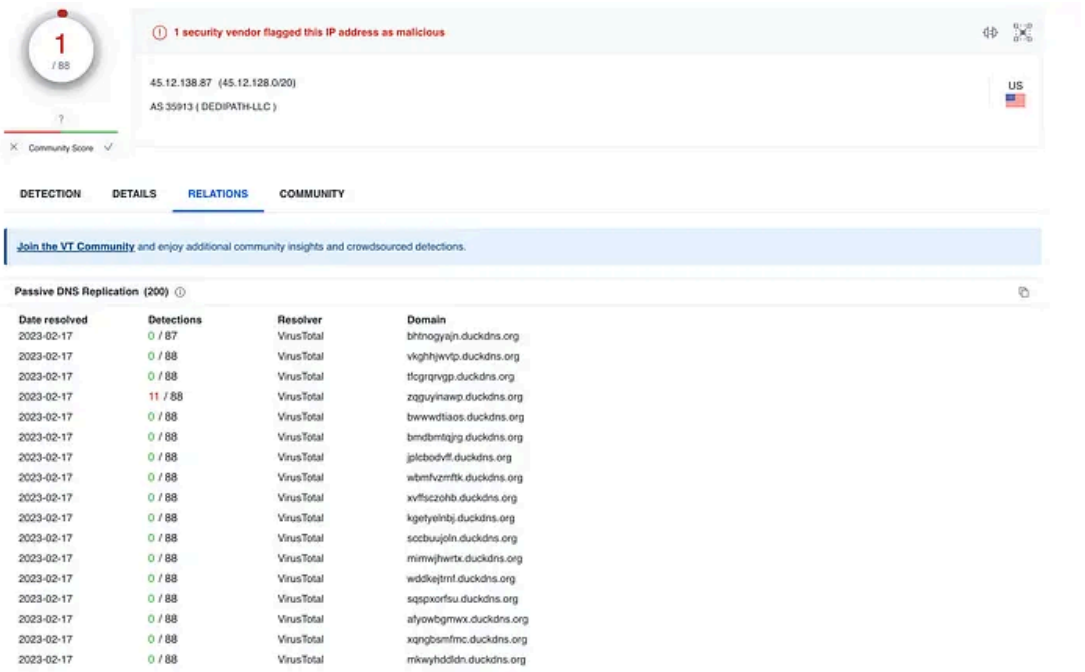
The second link's redirect will also change every few mins-hours.

Press enter or click to view image in full size



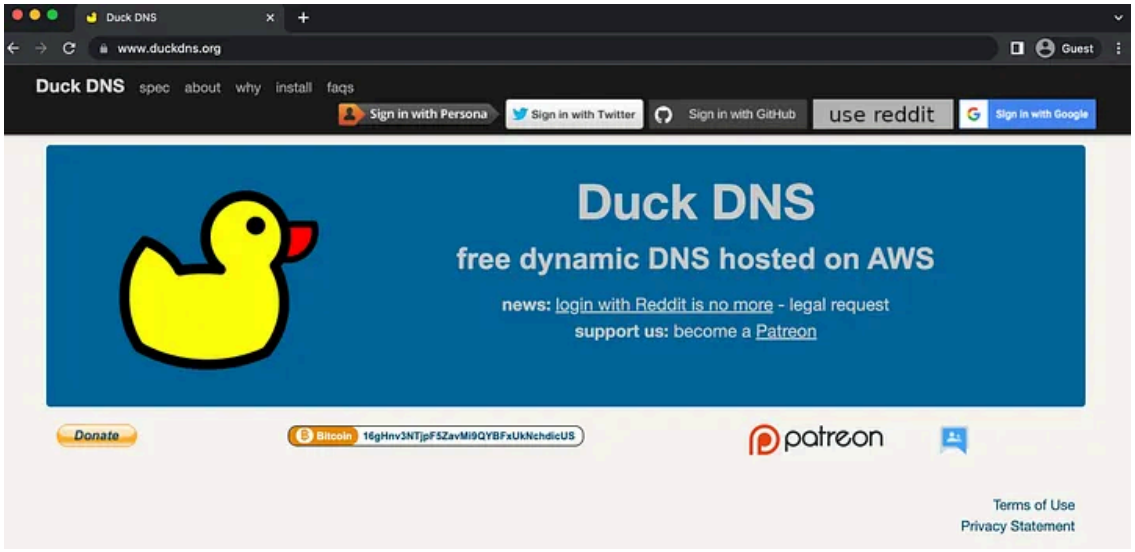
The first and second Duck DNS domain has an IP of 45.12.138[.]87, and has many Duck DNS domains associated with them.

Press enter or click to view image in full size



As Duck DNS is a free dynamic DNS, it is often abused for malicious purposes like in this case.

Press enter or click to view image in full size



Conclusion

In this investigation, it was found that the behaviour of the smishing attack differs based on the User-Agent, and abuses Duck DNS. Multiple redirects are made before it reaches the fake AU page. Accesses from certain locations will prevent the fake AU page from loading.

- Android User-Agent: Redirects the user to a fake AU page, and downloads a malicious file called `KDDI.apk`
- iPhone User-Agent: Redirects the user to a fake AU page, and asks for the user's details, and Vプリカ (prepaid card) numbers.

The behaviour of this smishing attack is similar to the one analyzed in my other blog, where it abused Duck DNS and changed behavior based on the User-Agent.

So if you receive an SMS message that uses Duck DNS, please be careful!
