Identifying the Nexus of Scaled Ad Fraud

spur.us/identifying-the-nexus-of-scaled-ad-fraud/

Riley Kilmer May 17, 2023

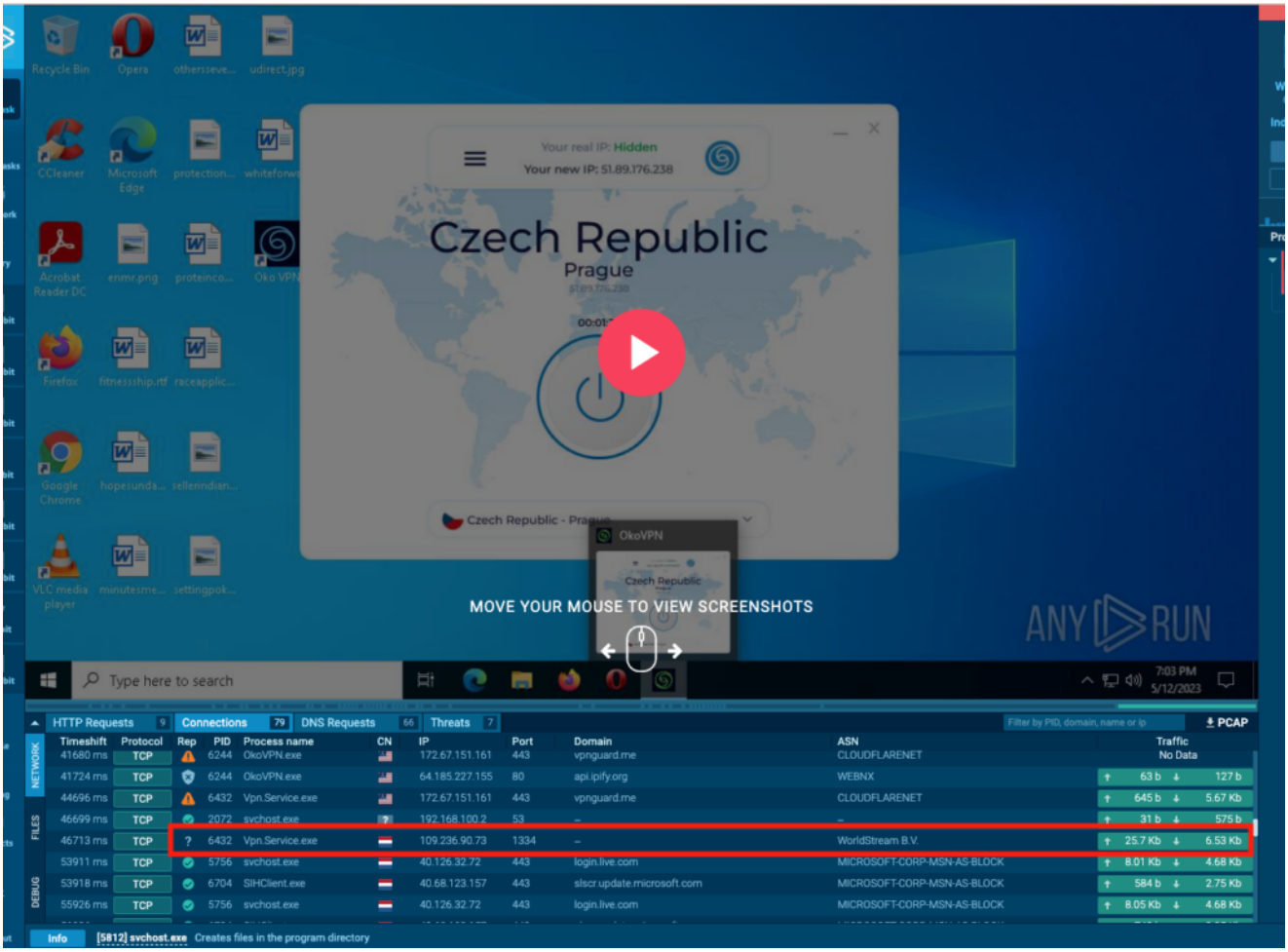
The Problem

Late last week, I was ~~procrastinating~~ perusing LinkedIn and encountered an article that referenced a scaled ad-fraud campaign powered by a free VPN application called Oko VPN (okovpn[.]com). The second I saw the article title, I had a gut feeling it had to involve a residential proxy service. First, I wanted to know if that was true. Second, was it a service we already track? Unfortunately, the article stopped short of identifying which service fueled the reported fraud.

I had to know…

The Journey Begins

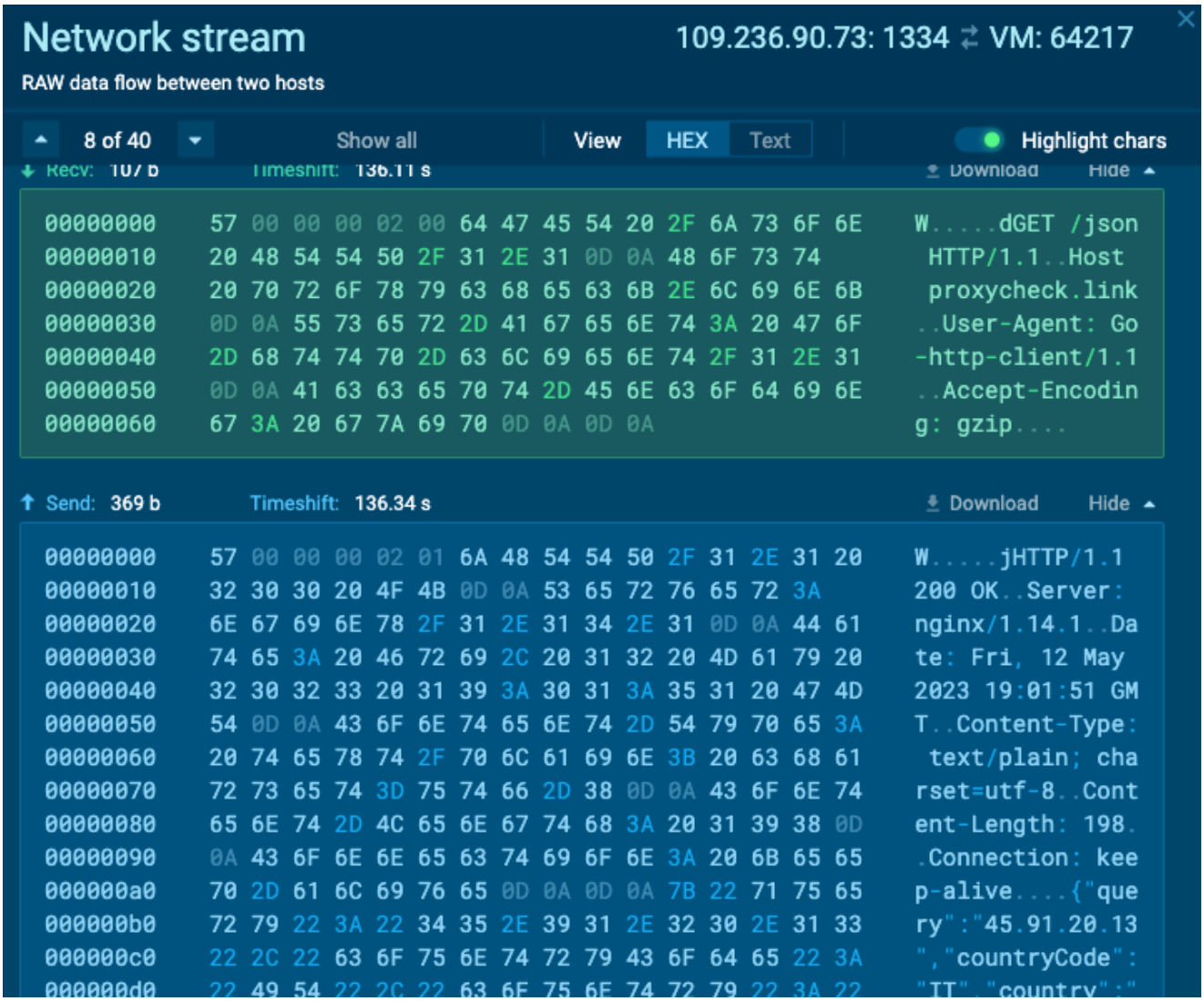
Since there were not any real indicators of compromise (IOCs) provided by the article, I set out to find them. The best way to determine which service is utilizing Oko is identifying the backend callback infrastructure. I noticed they had a Windows application which makes this trivial to check. After a few minutes in Any.Run, we were off to the races. You can look at the Any.Run report here.



The IP address `109.236.90.73` really stood out to me during this analysis. It is an odd port and no associated domain within the sandbox. Using my DNSDB CLI from DomainTools, I found some interesting domains.

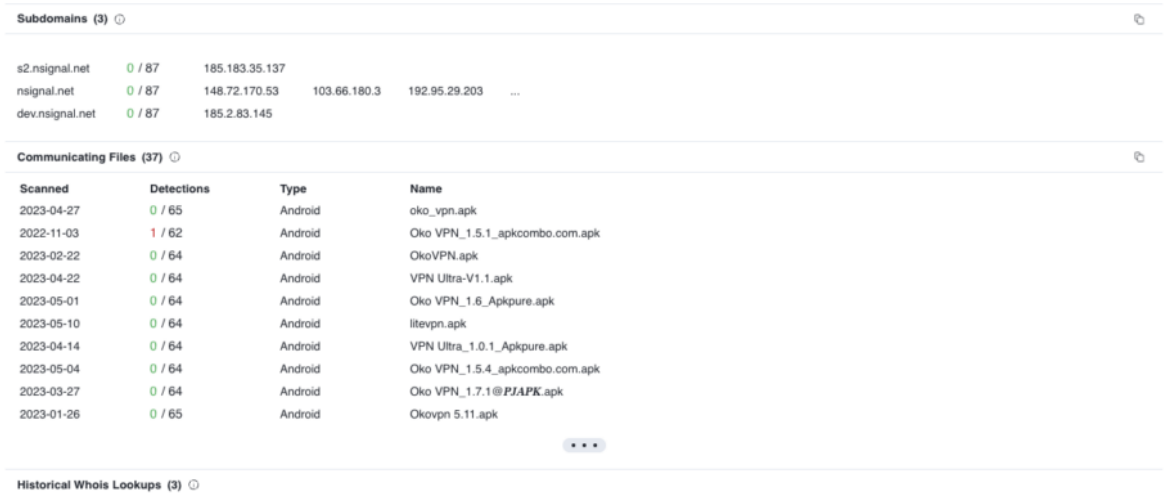
```
➜  ~ dnsdb 109.236.90.73
109.236.90.73    2022-11-08T07:08:05Z    2023-05-16T13:24:58Z    nsignal.net.
109.236.90.73    2022-11-28T09:07:37Z    2023-05-16T11:02:11Z    ts13.p2proxy.net.
109.236.90.73    2022-11-08T15:55:56Z    2023-05-16T03:03:05Z    109-236-90-
73.hosted-by-worldstream.net.
```

`p2proxy[.]net` and `nsignal[.]net` both look like very likely candidates. But before diving deeper into these domains, I wanted to look at the contents of this TCP stream.



This definitely looks like plain-text proxying through my sandbox to check IP address information. Before long, there was a TLS connection made using this tunnel to Instagram and other services using this same TCP tunnel. This information really affirmed my thought that this host was the responsible command-and-control for the residential proxy service. Unfortunately, `nsignal[.]net` nor `p2proxy[.]net` were associated with any of the services we already track.

Sometimes, these IOCs are easy to track back to the associated services. Unfortunately, simple Google searches only yielded results from years ago connecting to some blockchain proxy pool. VirusTotal searches for `nsignal[.]net` only yielded more OkoVPN samples. Investigations into this infrastructure were fairly frustrating and did not yield any hints as to which network was reselling this bandwidth.



Subdomains (3)

s2.nsignal.net	0 / 87	185.183.35.137			
nsignal.net	0 / 87	148.72.170.53	103.66.180.3	192.95.29.203	...
dev.nsignal.net	0 / 87	185.2.83.145			

Communicating Files (37)

Scanned	Detections	Type	Name
2023-04-27	0 / 65	Android	oko_vpn.apk
2022-11-03	1 / 62	Android	Oko VPN_1.5.1_apkcombo.com.apk
2023-02-22	0 / 64	Android	OkoVPN.apk
2023-04-22	0 / 64	Android	VPN Ultra-V1.1.apk
2023-05-01	0 / 64	Android	Oko VPN_1.6_Apkpure.apk
2023-05-10	0 / 64	Android	litevpn.apk
2023-04-14	0 / 64	Android	VPN Ultra_1.0.1_Apkpure.apk
2023-05-04	0 / 64	Android	Oko VPN_1.5.4_apkcombo.com.apk
2023-03-27	0 / 64	Android	Oko VPN_1.7.1@*PJAPK*.apk
2023-01-26	0 / 65	Android	Okovpn 5.11.apk

Historical Whois Lookups (3)

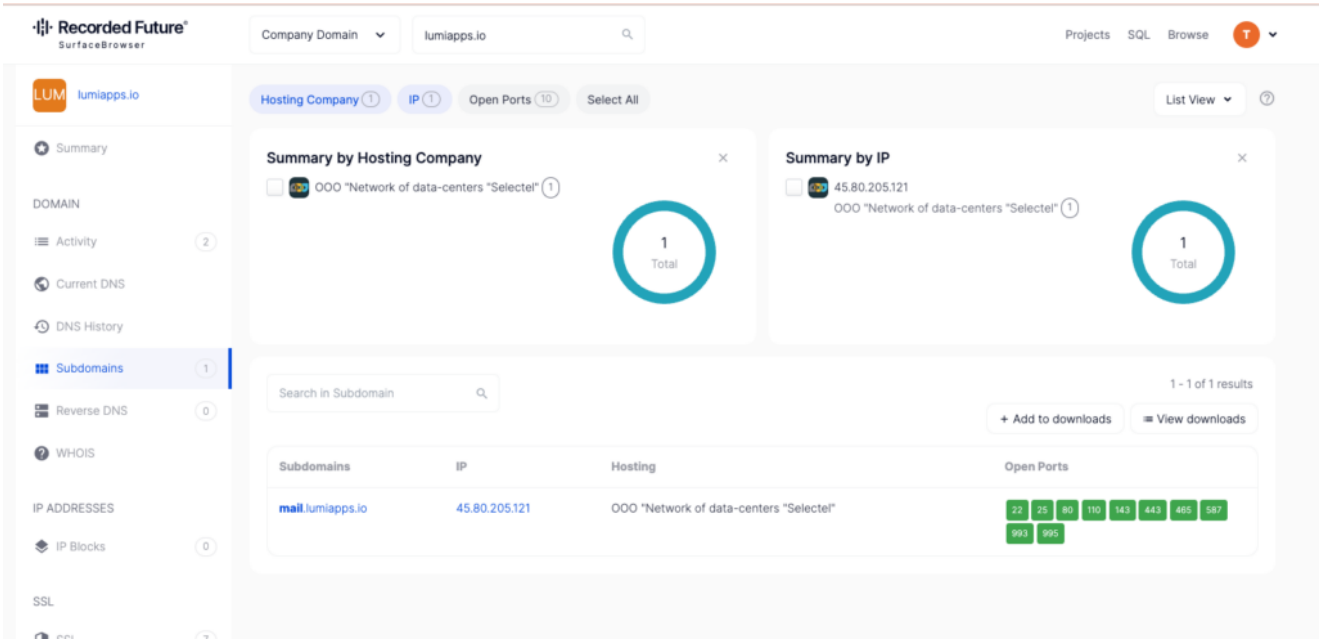
Back to the beginning

Our only real connection to this mystery network was Oko VPN. There is always the possibility that the VPN itself is owned by the service directly. If this is the case, the terms of service and/or privacy policy can be very revealing. I didn't even reach the end of the terms of service before I was met with a revelation:

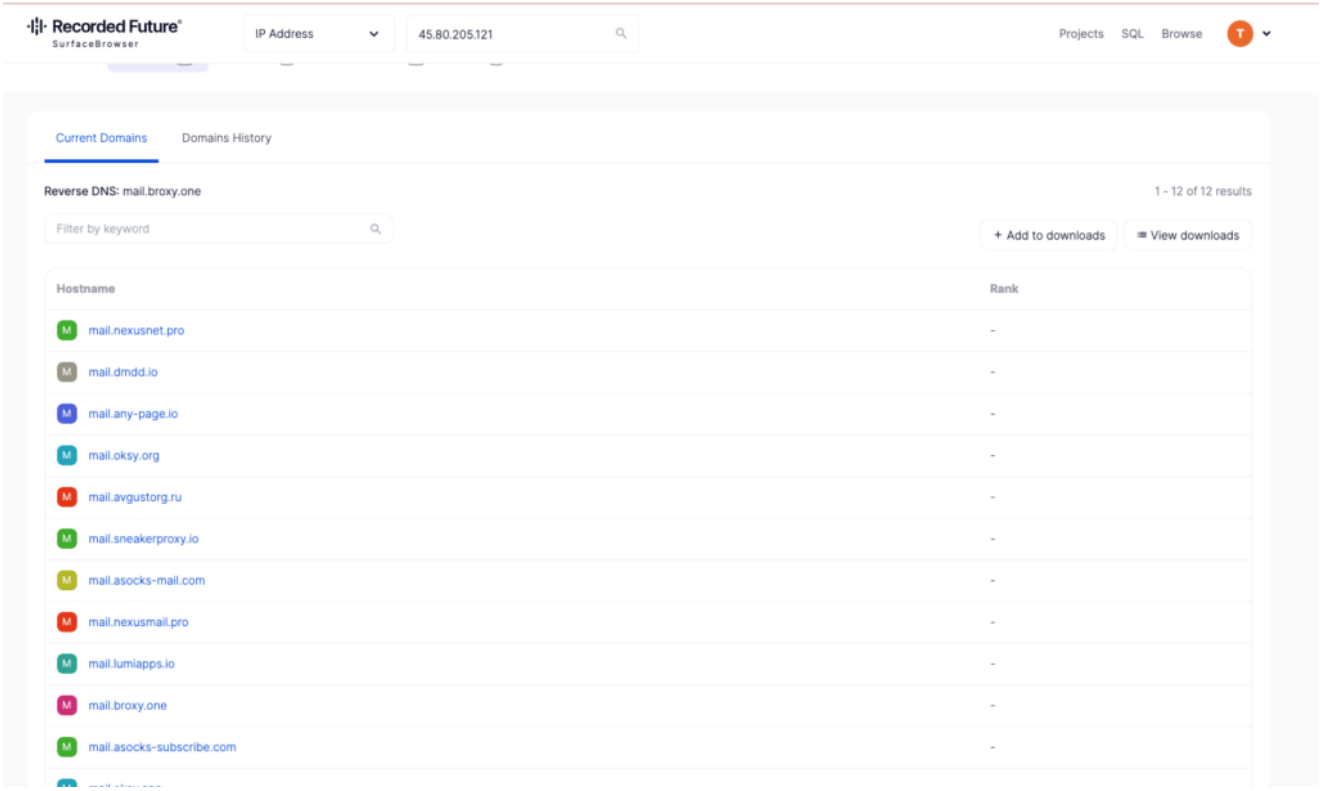
```
In return for some of the premium features of "Oko VPN', you may choose to be a peer
on the
D.M.D.D. network. By doing so you agree to have read and accepted the Terms of
Service of the
D.M.D.D.'s SDK EULA: https://lumiapps.io/End_User_License_Agreement.pdf
and D.M.D.D.'s Privacy Policy: https://lumiapps.io/DMDD_SDK_Privacy_Policy.pdf.
You may opt out of the D.M.D.D.'s network by clicking: Personal settings => switch
the
tubler of => agree that you want to cancel your participation in D.M.D.D. network.
```

We have talked a lot about how different residential proxies source their IP addresses. Many of these free VPN apps play the game of embedding consent deep within their TOS or privacy policies. The lumiapps[.]io website did not have any obvious answer. I was really hoping for some area titled "Want to buy bandwidth from us?" or similarly phrased section. But now we have a handful of clues and hopefully one of these domains or IP addresses they are using links them to a residential proxy service.

SurfaceBrowser by Recorded Future is one of my favorite tools for just throwing spaghetti at the wall. I saw a subdomain that looked really promising. Or at least pretty suspect. The mail server being hosted in Russia definitely felt like a clue worth pursuing.



Pivoting on the IP address `45.80.205[.]121` led me to a whole lot of other mail servers that could definitely be the culprits.



When I showed this to my research team, one of my teammates was quick to saying “I have heard of NexusNet”. Their primary service is operated at `nexusnet[.]io`. This service was on a list we were actively investigating for addition to our tracking system.

After a couple of hours of enumeration, we had a list of NexusNet proxies. Using our android sandbox environment running a longer job of Oko VPN, we were able to see our activity within our own sandbox using the `nsignal[.]net` tunnel. This was the last piece of evidence that helped us tie up this investigation.

Conclusion

If a VPN service is free and claiming no-logs, there has to be a catch. Whether that is advertisements or other monetization like bandwidth re-selling, you are the product. Installing Oko VPN on your device would have included your IP address in this reported Ad fraud campaigns or any other fraud being performed by customers of NexusNet.

Take a look at our active intelligence on NexusNet using our community dashboard. And if you are looking for ways to prevent these networks from abusing your platforms, check out our feeds, API tools, and Monocle.