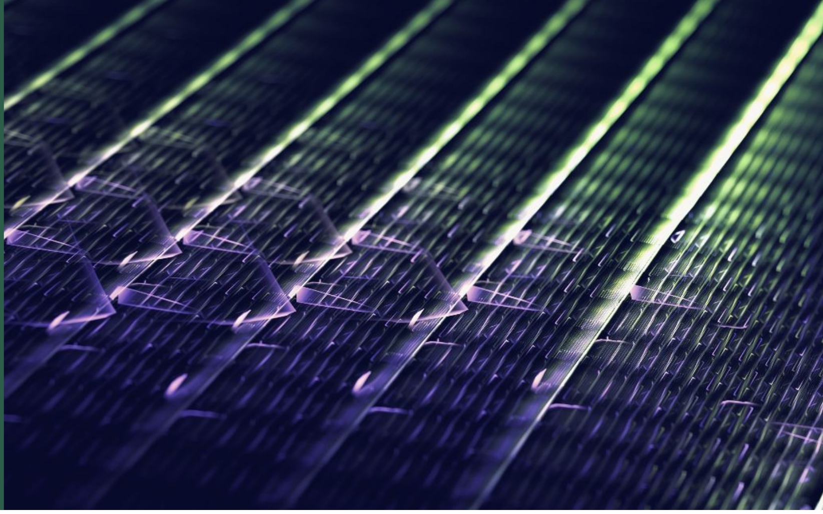
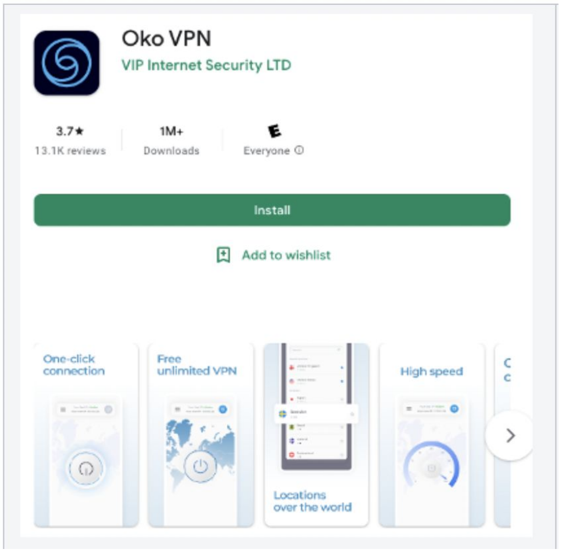
IAS

IAS THREAT LAB

TECHNICAL DISCLOSURE: OKO VPN



Integral Ad Science has uncovered a malicious VPN app with over one million downloads that hijacks residential IPs for ad fraud



GOOGLE PLAY STORE

1 million+ installs

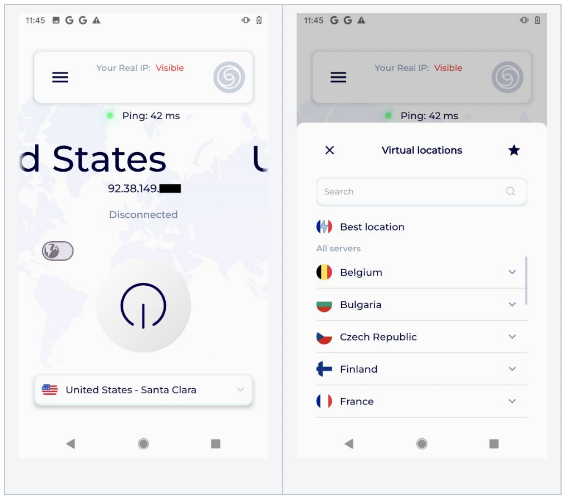
BACKGROUND STORY

Integral Ad Science (IAS) identified a malicious app that surreptitiously converts users' mobile devices into proxies for ad fraud. The estimated waste to advertiser spend is $2M per month in fraudulent video ad inventory.

Oko VPN app, a free-to-download, free-to-use app available on multiple app stores including Google Play, allows users to disguise their IP addresses to servers across the world.

Available for download since July 2022, Oko has experienced exponential growth, with half a million users in late November 2022 and over a million at the time of its takedown in March 2023.

Oko VPN's user base is predominantly in the United States, Germany, and Russia. However, it is used worldwide.



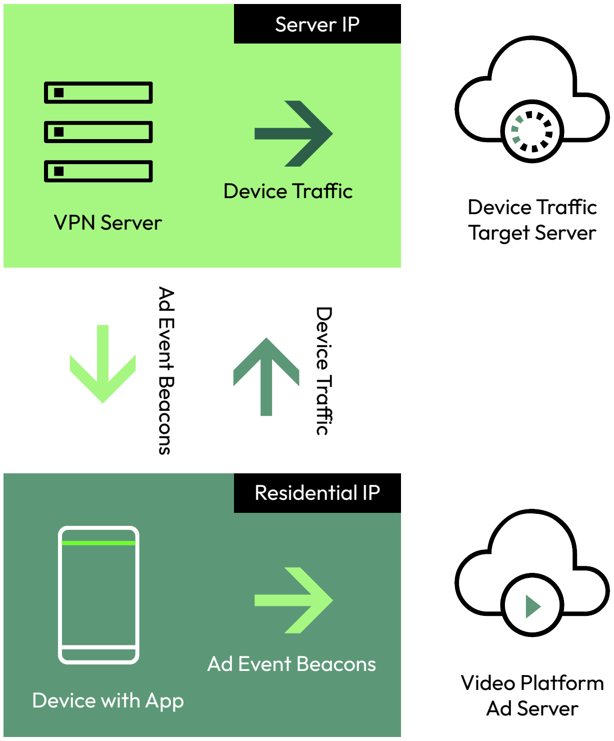
OKO VPN App

BACKGROUND STORY

Oko VPN's free service comes with a hidden cost. Unbeknownst to its users, the app contains malicious code that turns a user's phone into a relay for fraudulent traffic. While you are disguising your identity and traffic through Oko VPN's server IPs, Oko VPN is disguising its ad traffic through your IP!

Users who download Oko VPN unwittingly donate their residential IP addresses for use by the app's operators. Oko VPN's operators use donated IPs to make server-based fraudulent ad traffic appear to originate from real human users behind residential IPs.

Oko VPN users also put themselves at risk of relaying email traffic. Technically, any TCP or UDP traffic may be relayed through donated IPs. This opens up IP donors to potential liability for illicit traffic that flows through their respective networks.



OTHER RESIDENTIAL IP HIJACKINGS SCHEMES

For those familiar with residential IP proxy networks, Oko VPN may bring to recollection HolaVPN and VIP72 (Bunitu). Both networks offered residential IP addresses for rent, and their methods for IP acquisition bordered on legal to illicit.

HolaVPN carries a reputation of being a community-based IP share system. HolaVPN users donate their IPs to a pool of addresses assuming that they will obtain another address from the shared pool. According to Trend Micro, the majority use case for donated residential IP addresses may likely have pertained to ad fraud.

VIP72 (Bunitu)	https://www.theregister.com/2015/08/11/bunitu_botnet_vpn_scam/
HolaVPN	https://web.archive.org/web/20210227012527/www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/shining-a-light-on-the-risks-of-holavpn-and-luminati
RSOCKS	https://krebsonsecurity.com/2022/06/meet-the-administrators-of-the-rsocks-proxy-botnet/

Trend Micro faced a defamation lawsuit filed by the owners of Luminati Networks (Hola VPN's handler company)
https://unicourt.com/case/ca-scl-luminati-networks-ltd-vs-trend-micro-inc-1112501

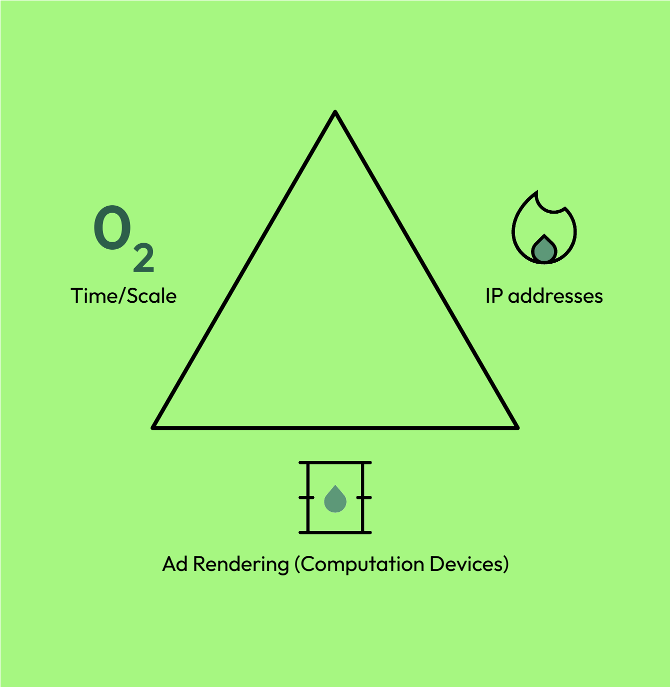
THE VALUE OF UNIQUE AND DIVERSE IP ADDRESSES

Think of ad operations (and ad fraud operations) as you would a fire. A vibrant fire requires three key ingredients: oxygen, fuel, and ignition.

A vibrant organic ad operation also requires three key ingredients:

- Computation assets for ad event rendering
- Unique residential IP addresses for ad event beaconing
- Time (or scale)

Akin to effective organic ad operations, effective ad fraud operations also require a diverse array of residential IP addresses... or proxies.



USE IN AD FRAUD

Similar to many other residential IP hijacking schemes, the residential IP network cultivated by Oko VPN appeared to deal heavily in ad fraud.

Of the traffic that was observed to pass through compromised devices, the majority was directed at video streaming platforms.

Interestingly, video ad traffic was observed to have been unaccompanied by content video. In other words, advertisement beacons were proxied through compromised devices, but content video streams were not.

Oko VPN operators' may have opted for this design decision as:

- Victim video platforms may not verify if ad beacons were fired from within the same contexts as those of content video requests. In other words, platforms may not verify if the IP addresses firing ad beacons were the same addresses requesting content video from CDNs.
- Oko VPN operators were conscious of the need to minimize mobile data and power drainage on victim devices in order to evade detection.

USE IN AD FRAUD CONT.

Another noteworthy pattern we observed was the scarcity of ad beacons fired from devices on any given day. Regardless of if the app was actively tunneling user traffic or laying dormant in the background, only a handful of video ad beacon traffic was observed daily.

This scarce utilization of compromised IPs is not an oddity when it comes to residential proxy-based fraud. If a network of hijacked residential IPs is of any substantial size, operators may be highly selective in to how they employ addresses. Common modus operandi is to minimize the use of any single IP address so as not to draw attention to it (so as to avoid IP based blocking).

This is a hallmark example of the more sophisticated ad fraud techniques that our industry faces today.

More transparent standards, monitoring and industry-wide information sharing are critical to combat this type of growing threat.

IMPACT ESTIMATE

We estimate that Oko VPN was generating approximately 100 million fraudulent impressions per month at the time of its takedown from the Google Play Store.

This equates to $2 million per month in wasted advertiser spend at a $20 video CPM rate.

SOLUTION

- The IAS Threat Lab team collaborated with the Google Play Store team on the takedown.
- On March 23, 2023, Google removed the app and enforced Google Play Protect, which warns users and prompts them to uninstall the malicious app.
- The IAS Threat Lab team has contacted affected video platforms to provide assistance in building stronger checks against threats like those posed by Oko VPN.