Big Socks to Fill: Tracking the Next 911RE

spur.us/big-socks-to-fill-tracking-the-next-911re/

Riley Kilmer

September 27, 2022

Someone Call 911: A Proxy Service Died

It's been over two months since the malware proxy service 911re imploded and there have been no clear frontrunners to fill the void. A few contenders looked up to the task, SocksEscort and Yilu Proxy, but SocksEscort quickly closed their doors to new sign-ups (likely in an effort to remain under the radar) while Yilu has faced difficulties with usability, payments, and pricing.

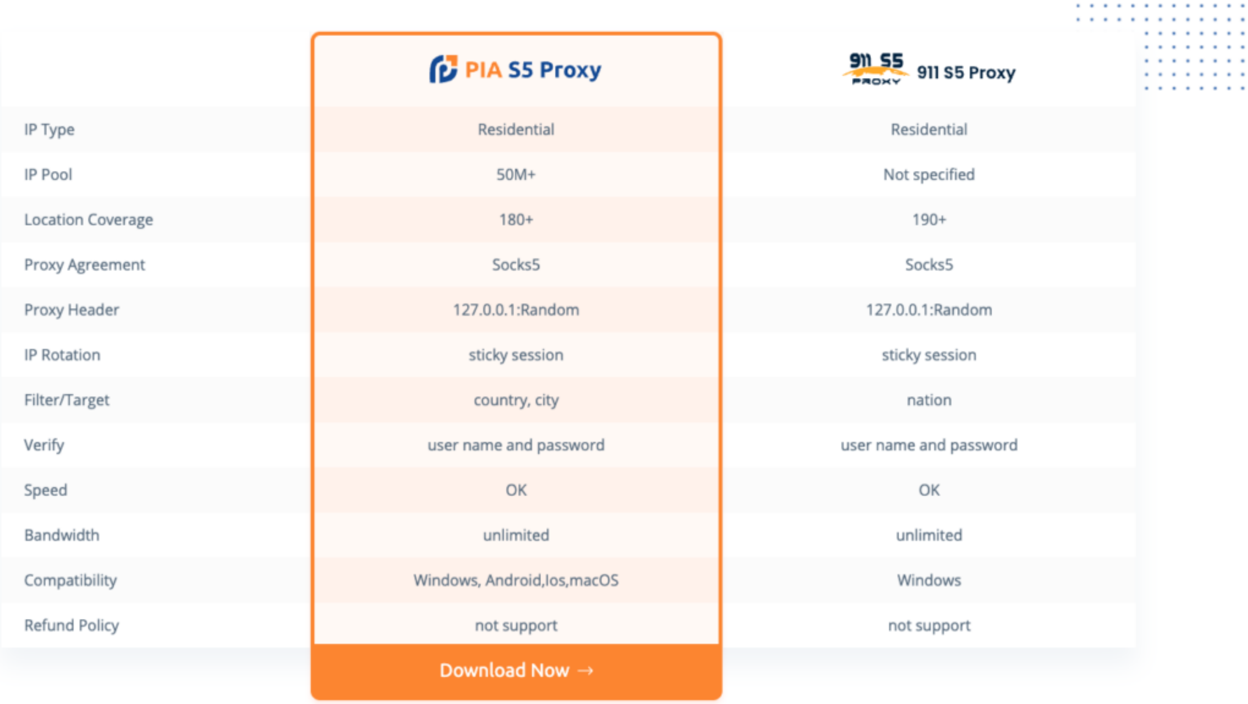
911 offered a convenient and familiar way to pay for proxies; similar to defunct services Luxsocks and VIP72, customers could purchase individual proxies with highly specific regionality and ISP requirements via a custom Windows application. SocksEscort and Faceless (yet another malware proxy service) offer similar functionality through a web interface but do not have the ease of use in native Windows environments.

Meanwhile, Yilu *does* have a Windows application but requires payment through WebMoney or USDT-TRON as opposed to more popular payment methods like BTC or ETH. Adding to its drawbacks, Yilu charges for bandwidth (as opposed to a flat daily rate for an IP) which can get very expensive, and ultimately the service looks to be a combination of multiple other services.

In this blog, we're going discuss how a new contender aims to replace 911 while still having familiar ties to an existing proxy service.

Enter: PIA S5 Proxy

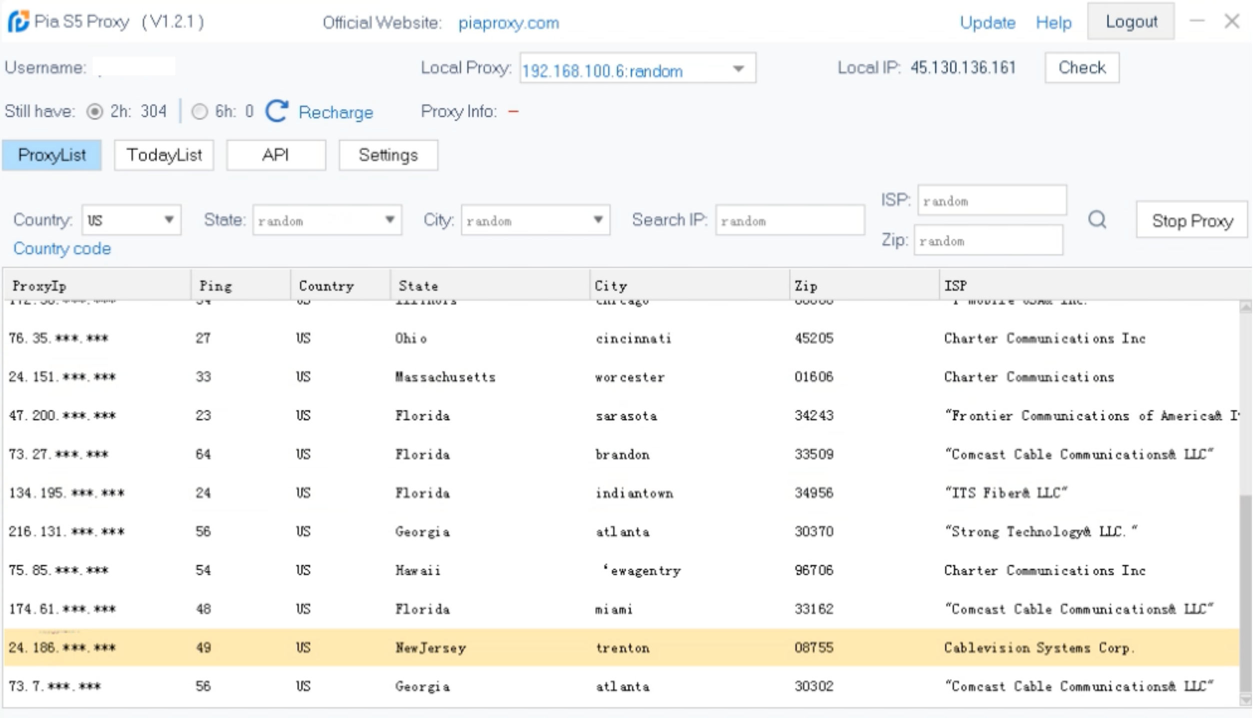
While investigating a mobile VPN application called IPChanger, Spur discovered a new proxy service: PIA S5 Proxy. This service specifically markets itself to ex-911 users.



	PIA S5 Proxy	911 S5 Proxy
IP Type	Residential	Residential
IP Pool	50M+	Not specified
Location Coverage	180+	190+
Proxy Agreement	Socks5	Socks5
Proxy Header	127.0.0.1:Random	127.0.0.1:Random
IP Rotation	sticky session	sticky session
Filter/Target	country, city	nation
Verify	user name and password	user name and password
Speed	OK	OK
Bandwidth	unlimited	unlimited
Compatibility	Windows, Android,Ios,macOS	Windows
Refund Policy	not support	not support

PIA S5 compared with 911re – Speed: OK, refunds: not OK

Users of 911 would feel right at home in the PIA interface, which is uncannily similar. Geographic and ISP targeting is possible when purchasing individual IPs, a common theme among malware proxy services like 911.



Pia S5 Proxy (V1.2.1) Official Website: piaproxy.com

Username:

Local Proxy: 192.168.100.6:random

Local IP: 45.130.136.161

Still have: ● 2h: 304 ○ 6h: 0

Proxy Info: –

Country: US State: random City: random Search IP: random ISP: random Zip: random

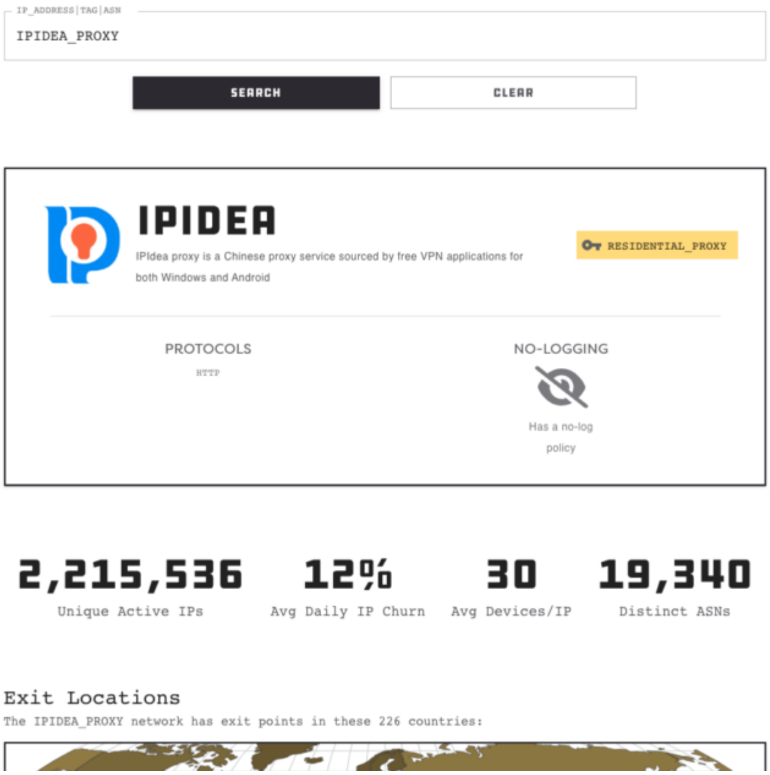
ProxyIp	Ping	Country	State	City	Zip	ISP
76.35.***.***	27	US	Ohio	cincinnati	45205	Charter Communications Inc
24.151.***.***	33	US	Massachusetts	worcester	01606	Charter Communications
47.200.***.***	23	US	Florida	sarasota	34243	"Frontier Communications of America& I
73.27.***.***	64	US	Florida	brandon	33509	"Comcast Cable Communications& LLC"
134.195.***.***	24	US	Florida	indiantown	34956	"ITS Fiber& LLC"
216.131.***.***	56	US	Georgia	atlanta	30370	"Strong Technology& LLC."
75.85.***.***	54	US	Hawaii	‘ewagentry	96706	Charter Communications Inc
174.61.***.***	48	US	Florida	miami	33162	"Comcast Cable Communications& LLC"
24.186.***.***	49	US	NewJersey	trenton	08755	Cablevision Systems Corp.
73.7.***.***	56	US	Georgia	atlanta	30302	"Comcast Cable Communications& LLC"

PIA S5 User Interface bears a striking similarity to 911

Spur has analyzed a number of PIA's proxy offerings and concluded these devices *also* belong to the IPIDEA residential proxy network. It seems apparent that PIA and IPIDEA share a common provenance or operator.

Pulling the thread

Spur has been tracking IPIDEA for a few months. Our analysis shows that they are fairly massive as far as residential proxy services go, with over 2.2m active IPs at the time of writing.



IP_ADDRESS | TAG | ASN

IPIDEA_PROXY

IPIDEA

IPIdea proxy is a Chinese proxy service sourced by free VPN applications for both Windows and Android

RESIDENTIAL_PROXY

PROTOCOLS

HTTP

NO-LOGGING

Has a no-log policy

2,215,536 Unique Active IPs

12% Avg Daily IP Churn

30 Avg Devices/IP

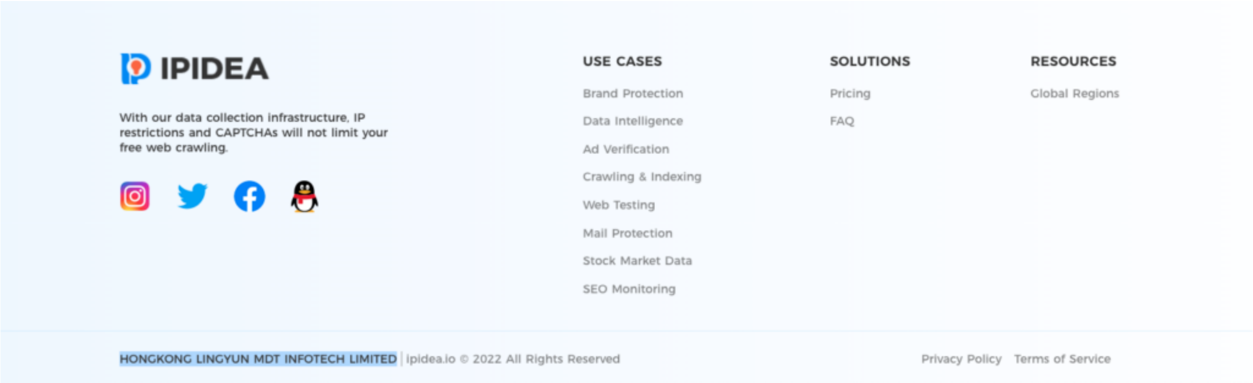
19,340 Distinct ASNs

Exit Locations

The IPIDEA_PROXY network has exit points in these 226 countries:

IPIDEA details on the Spur Dashboard

As it is not uncommon to find multiple residential proxy services “sharing” an IP, Spur continued to dig into both IPIDEA and PIA S5 Proxy to find additional details that could link them together. To start, we identified the corporate entity operating IPIDEA from their own website: `HongKong Lingyun MDT Infotech Limited`.



IPIDEA

With our data collection infrastructure, IP restrictions and CAPTCHAs will not limit your free web crawling.

USE CASES

- Brand Protection
- Data Intelligence
- Ad Verification
- Crawling & Indexing
- Web Testing
- Mail Protection
- Stock Market Data
- SEO Monitoring

SOLUTIONS

- Pricing
- FAQ

RESOURCES

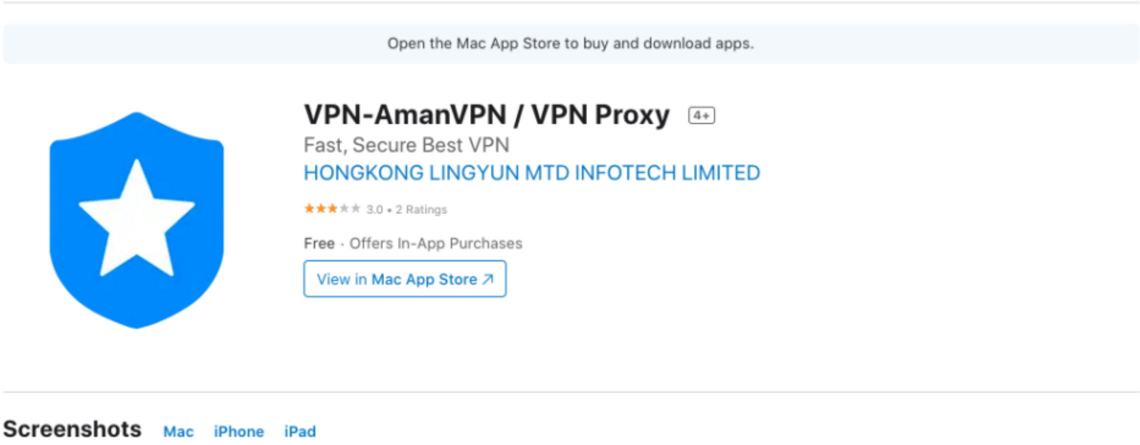
- Global Regions

HONGKONG LINGYUN MDT INFOTECH LIMITED | ipidea.io © 2022 All Rights Reserved

Privacy Policy Terms of Service

Footer from IPIDEA’s website showing ownership

Pivoting on that company name, we identified a VPN service for Android and iOS called AmanVPN. From the app store, we can see it is supposedly operated by the same company as IPIDEA.



Open the Mac App Store to buy and download apps.

VPN-AmanVPN / VPN Proxy 4+

Fast, Secure Best VPN

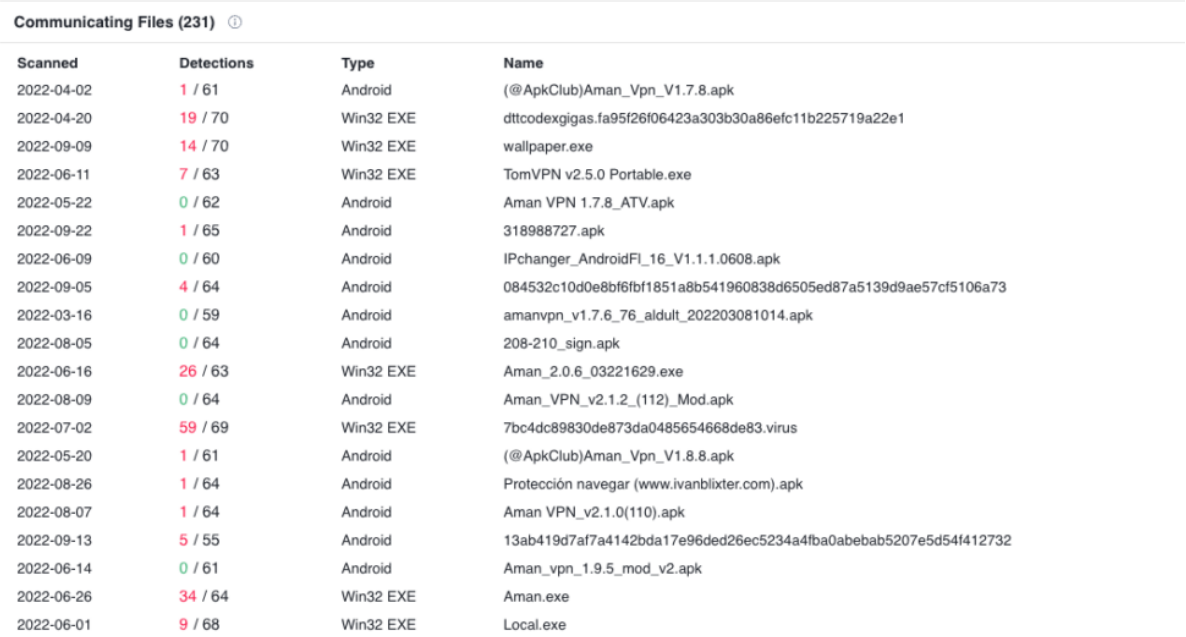
HONGKONG LINGYUN MTD INFOTECH LIMITED

★★★☆☆ 3.0 • 2 Ratings

Free · Offers In-App Purchases

AmanVPN in the App Store

Through dynamic analysis, AmanVPN was determined to be a "free" VPN app that helps IPIDEA source the proxies in their network. The domain `bazh.na.lb.holadns[.]com` appears to point to the callback infrastructure for their residential device pool.

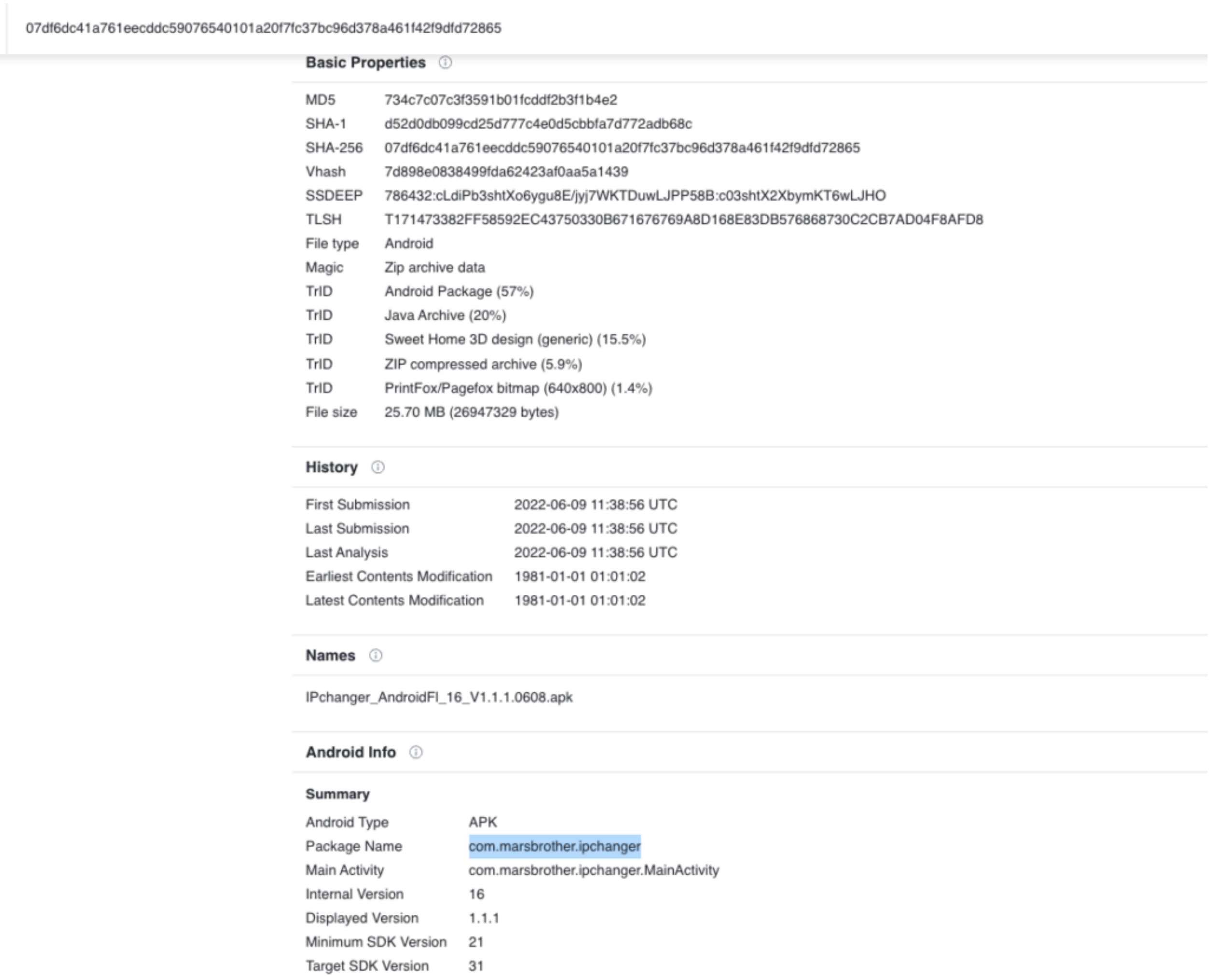


Communicating Files (231)

Scanned	Detections	Type	Name
2022-04-02	1 / 61	Android	(@ApkClub)Aman_Vpn_V1.7.8.apk
2022-04-20	19 / 70	Win32 EXE	dttcodexgigas.fa95f26f06423a303b30a86efc11b225719a22e1
2022-09-09	14 / 70	Win32 EXE	wallpaper.exe
2022-06-11	7 / 63	Win32 EXE	TomVPN v2.5.0 Portable.exe
2022-05-22	0 / 62	Android	Aman VPN 1.7.8_ATV.apk
2022-09-22	1 / 65	Android	318988727.apk
2022-06-09	0 / 60	Android	IPchanger_AndroidFl_16_V1.1.1.0608.apk
2022-09-05	4 / 64	Android	084532c10d0e8bf6fbf1851a8b541960838d6505ed87a5139d9ae57cf5106a73
2022-03-16	0 / 59	Android	amanvpn_v1.7.6_76_aldult_202203081014.apk
2022-08-05	0 / 64	Android	208-210_sign.apk
2022-06-16	26 / 63	Win32 EXE	Aman_2.0.6_03221629.exe
2022-08-09	0 / 64	Android	Aman_VPN_v2.1.2_(112)_Mod.apk
2022-07-02	59 / 69	Win32 EXE	7bc4dc89830de873da0485654668de83.virus
2022-05-20	1 / 61	Android	(@ApkClub)Aman_Vpn_V1.8.8.apk
2022-08-26	1 / 64	Android	Protección navegar (www.ivanblixter.com).apk
2022-08-07	1 / 64	Android	Aman VPN_v2.1.0(110).apk
2022-09-13	5 / 55	Android	13ab419d7af7a4142bda17e96ded26ec5234a4fba0abebab5207e5d54f412732
2022-06-14	0 / 61	Android	Aman_vpn_1.9.5_mod_v2.apk
2022-06-26	34 / 64	Win32 EXE	Aman.exe
2022-06-01	9 / 68	Win32 EXE	Local.exe

VirusTotal list of applications that share infrastructure with the AmanVPN mobile app

As seen in the VirusTotal output above, IPChanger — another Android VPN app — calls back to the same infrastructure used by AmanVPN. Looking at the APK information for IPChanger shows a package name of `com.marsbrother.ipchanger`



07df6dc41a761eecddc59076540101a20f7fc37bc96d378a461f42f9dfd72865

Basic Properties

MD5	734c7c07c3f3591b01fcddf2b3f1b4e2
SHA-1	d52d0db099cd25d777c4e0d5cbbfa7d772adb68c
SHA-256	07df6dc41a761eecddc59076540101a20f7fc37bc96d378a461f42f9dfd72865
Vhash	7d898e0838499fda62423af0aa5a1439
SSDEEP	786432:cLdiPb3shtXo6ygu8E/jyj7WKTDuwLJPP58B:c03shtX2XbymKT6wLJHO
TLSH	T171473382FF58592EC43750330B671676769A8D168E83DB576868730C2CB7AD04F8AFD8
File type	Android
Magic	Zip archive data
TrID	Android Package (57%)
TrID	Java Archive (20%)
TrID	Sweet Home 3D design (generic) (15.5%)
TrID	ZIP compressed archive (5.9%)
TrID	PrintFox/Pagefox bitmap (640x800) (1.4%)
File size	25.70 MB (26947329 bytes)

History

First Submission	2022-06-09 11:38:56 UTC
Last Submission	2022-06-09 11:38:56 UTC
Last Analysis	2022-06-09 11:38:56 UTC
Earliest Contents Modification	1981-01-01 01:01:02
Latest Contents Modification	1981-01-01 01:01:02

Names

IPchanger_AndroidFl_16_V1.1.1.0608.apk

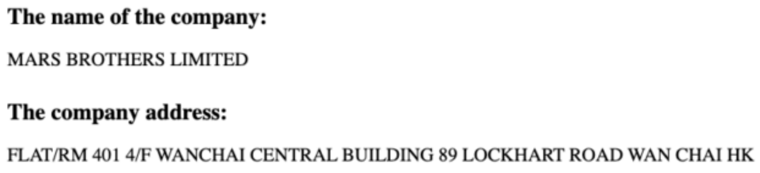
Android Info

Summary

Android Type	APK
Package Name	com.marsbrother.ipchanger
Main Activity	com.marsbrother.ipchanger.MainActivity
Internal Version	16
Displayed Version	1.1.1
Minimum SDK Version	21
Target SDK Version	31

IPChanger’s APK information in VirusTotal

This leads us back to PIA. As seen in the privacy policy on their website, PIA’s owner is `Mars Brothers Limited`. These connections between PIA and IPIDEA — in addition to sharing residential devices — leads us to the conclusion that they are ultimately operated by the same entity or at the very least white-labeling the “root” proxy service, likely IPIDEA.



The name of the company:

MARS BROTHERS LIMITED

The company address:

FLAT/RM 401 4/F WANCHAI CENTRAL BUILDING 89 LOCKHART ROAD WAN CHAI HK

Privacy Policy snippet from PIA S5 Proxy showing Mars Brothers ownership

Another day, another proxy

Unfortunately for security teams combating fraud and abuse on the Internet, this means the current replacement for 911 is *at least* 3x as large as 911 ever was. The pricing for PIA is roughly the same and their method of payment is very flexible. They support many types of cryptocurrencies with no KYC policies. We fully expect to continue to see abuse coming from this service. Luckily, Spur is already well positioned to alert our customers in real-time to IPIDEA’s large and ever-shifting residential proxy network. Contact sales@support.us to see how our real-time feeds or Monocle integration can help.