

CloudRouter: 911 Proxy Resurrected

 spur.us/cloudrouter-911-proxy-resurrected/

Sean S.

February 22, 2024

It's a scary world out there for residential IPs; they are the key product of "underground" proxy services like Faceless, SocksEscort, NSocks, the defunct 911 Proxy, and now CloudRouter which we suspect has taken its place. But productization of residential IPs is not limited to scary dark web storefronts. There are a surprising number of legitimate "bandwidth sharing" applications enticing users to sub-lease their Internet connection for mere pennies per gigabyte, and an even more surprising number of users who are fine with this exchange. [We've talked about the market for residential IPs](#) ad nauseum, but it feels like the problem is only getting worse.

A modest proposal

Picture this scenario: you're out on the town and are approached by a man in a nice suit with a spiffy briefcase (which is surely full of important papers and not crackers). Exuding confidence and professionalism, he makes you an interesting offer. He happens to know the bartender at your favorite pub and says you can put a couple of free beers on his tab whenever you're in town. In exchange, he asks for the permission to use your phone to make a series of calls for his business endeavors. He assures you that all such calls will be completely legal, adhering to a stringent set of ethical standards he personally oversees. Additionally, he might occasionally allow a handful of his trusted business partners to use your phone number for their calls, also bound by the same rigorous guidelines.

Now, another scenario: Imagine you're walking down an empty street when a shadowy figure steps out from an alleyway, dressed in trench coat and with a mysterious shadow cast over his face, like the cliché antagonist from an old film noir flick. He subtly grabs your attention and makes you different offer. He presents you with a state-of-the-art smartphone, loaded with every app and feature you've ever wanted, no subscription fees, no one-time payments—completely free. But there's a catch.

In exchange for this dream device, the shadowy figure asks for the permission to use your new phone to make any calls he wants, anytime, without needing to inform you. He assures you that you won't even notice, that it'll be as if the calls never happened. But there's more—he also wants the freedom to let anyone he chooses use your phone number to make their calls, again without your direct knowledge.



It wouldn't be a blog post in 2024 without some gratuitous AI imagery

This analogy attempts to illustrate the surface-level difference between explicit bandwidth sharing apps (like EarnApp, Honeygain, Pawns, Repocket, Cash Raven, Pop, etc) and the countless “free VPN” apps like MaskVPN. The end result is mostly the same, but at least with the former you’ve got a vague idea of what your phone is being used for while you enjoy your “free” beer.

Bright Data (EarnApp) and Oxylabs (Honeygain) pay their peers the most—which is not much—and *generally* make an *attempt* to enforce KYC policies on their customers. To be clear, this is not an endorsement. The bar is just really low. Either way, your IP address, once a personal line to the world, can now be used in dealings you’re unaware of, for purposes unknown to you, and by people you’ve never met.

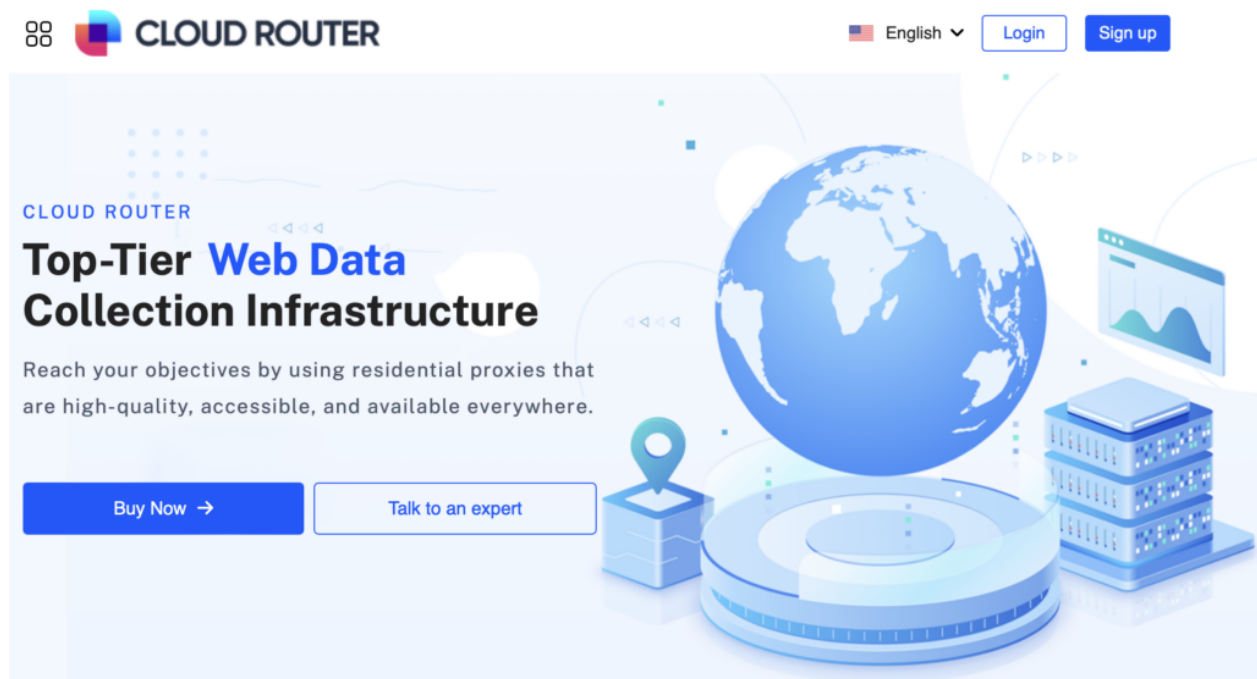
If you’re a reader of this blog, the dodgy nature of bandwidth sharing offers probably doesn’t need explaining. You’re not here to be told off for downloading and running questionable software that blatantly plans to monetize your IP address. But a significant portion of residential proxies stem from people who apparently see no problem with this exchange.

Will the real 911 Proxy, please stand up?

One such example was **MaskVPN**, whose users unknowingly contributed to the pool of IPs for the criminal proxy service **911.re** aka 911 Proxy—a service that went belly-up in the fall of 2022. Unsurprisingly, MaskVPN also disappeared shortly thereafter. Since then, the void left in the market has had a lot of attempted fillers, [some we’ve written about in the past](#). Do a Google search for “911 proxy” and you’ll find dozens of services claiming to be the best

replacement. This seems like a dubious accolade for most commercial proxy services who at least pretend to be on the level; 911 proxies (and thus MaskVPN users) were consistently responsible for large scale banking fraud and corporate ATO operations.

An interesting candidate to *actually* fill 911's shoes recently popped up on our radar: a residential proxy service known as **CloudRouter** that markets itself as having "high-quality" residential IPs that users can buy on a per-IP basis using a native Windows client. This was the modus operandi of 911.re. Our interest was immediately piqued, as residential proxy services tend to all look the same (web interface, rotating or static sessions, pay per gigabyte, etc). This one looked markedly different and yet *familiar*.



CloudRouter homepage

Upon downloading and executing the client, the similarity was unmistakable. Following a hunch, we checked out the network requests and sure enough, nothing had changed; all the API paths were identical. 911's back, baby, Voldemort-style. The legendary criminal proxy service has found its footing once again and resumed operations under a new name. Only one question remains: what app or apps are supplying the IPs for this new incarnation?

A rose by any other name

CloudRouter 1.0 Official Website: CloudRouter.io

Username: dodo Local Proxy: 192.168.187.253:19478 On Top
 Remaining: 4741 proxies Current Proxy: 108.167. (US OH Circleville)
 App Path: c:\program files\google\chrome\application\chrome.exe

Connections: 0 0.0 KB/s

Apps Proxies List Today's List Favorite Proxies Proxy API Settings

Country: US State: All City: All Start IP: 0.0.0.0 End IP: 0.0.0.0 ISP: All ZIP: All Stop proxy

Proxy IPs	Ping	Country	State	City	ZIP	ISP
172.***.***.***	53	US	NC	Fuquay Varina	27526	Spectrum
104.***.***.***	11	US	CA	Torrance	90503	Spectrum
73.***.***.***	18	US	WA	Renton	98056	Comcast Cable
66.***.***.***	38	US	MO	Saint Ann	63074	Spectrum
174.***.***.***	134	US	VA	Charlottesville	22911	Verizon Wireless
73.***.***.***	33	US	FL	Vero Beach	32962	Comcast Cable
71.***.***.***	47	US	PA	Reading	19605	Comcast Cable
174.***.***.***	18	US	WA	Seattle	98144	CenturyLink
108.***.***.***	42	US	GA	Roswell	30075	AT&T U-verse
185.***.***.***	51	US	NY	New York	10013	M247 Ltd
98.***.***.***	36	US	IL	Frankfort	60423	Comcast Cable
99.***.***.***	23	US	GA	Douglasville	30134	AT&T U-verse
104.***.***.***	7	US	CA	Woodland Hills	91367	Spectrum
174.***.***.***	52	US	KS	Emporia	66801	JMZCO
173.***.***.***	36	US	MO	Carl Junction	64834	Mediacom Cable
73.***.***.***	34	US	IL	Rockford	61101	Comcast Cable
69.***.***.***	35	US	MO	Blue Springs	64014	Comcast Cable
73.***.***.***	35	US	IL	Morton Grove	60053	Comcast Cable
24.***.***.***	35	US	NJ	Newark	07106	Optimum Online
12.***.***.***	5	US	AZ	Phoenix	85013	AT&T Services
24.***.***.***	37	US	NY	Manhasset	11030	Optimum Online
71.***.***.***	39	US	GA	Savannah	31401	Comcast Cable

Port Forward List WhiteList First Previous 1/955 Next Last Refresh

911 55 3.26 Official Website: 911.re Mirror: 911.gg 911s5.com

Username: donbrowser Local Proxy: 192.168.18.149:1000 Clear browser info Fill Form On Top
 Still have: 142 proxy Proxy Info: 205.206.202.212 (CA AB Edmonton) Using Server: US1-GIA
 Useragent: Default Change Server
 Screen Resolution: Default Application Path:

Program ProxyList TodayList FavoriteProxy UserAgent Referer PersonalData ConversionTrack AutoProxy BlockSites Settings

Country: All State: All City: All StartIP: 0.0.0.0 EndIP: 0.0.0.0 ISP: All Zip: All Auto Refresh 15 Minutes

ProxyIP	Ping	Country	State	City	Zip	ISP
190.***.***.***	124	PE	LMA	Lima		Telefonica del Peru
111.***.***.***	125	ID	JK	Jakarta		FirstMedia
94.***.***.***	145	GR	M	Heraklion		Cosmote
125.***.***.***	245	VN	SG	Ho Chi Minh City		Viettel Group
208.***.***.***	34	US	OH	Cincinnati	45244	Fuse Internet Access
64.***.***.***	36	US	AK	Wasilla	99687	MTA Solutions
14.***.***.***	39	JP	Unknow	Toyohashi	441-8101	JPNE
99.***.***.***	43	CA	ON	Toronto	M2M	Rogers Cable
72.***.***.***	60	JM	Unknow	Mandeville		FLOW
119.***.***.***	61	JP	Unknow	Unknow	020-0573	Biglobe
88.***.***.***	77	GB	ENG	Goole	DN14	TalkTalk
24.***.***.***	80	US	IL	Chicago	60640	Comcast Cable
82.***.***.***	81	GB	ENG	Stoke-on-Trent	ST4	Virgin Media
211.***.***.***	81	KR	Unknow	Cheonan	31132	Korea Telecom
188.***.***.***	82	ES	AN	Seville	41003	Vodafone Spain
89.***.***.***	87	LV	RIX	Riga	LV-1001	SIA Baltcom
80.***.***.***	88	ES	MD	Valdemoro	28341	Telefonica de Espana
93.***.***.***	93	DE	BY	Wurzburg	97076	Deutsche Telekom AG
86.***.***.***	95	RO	MS	Reghin	545300	Digi Romania
118.***.***.***	96	KR	Unknow	Mapo-gu	04365	SK Broadband
175.***.***.***	97	AU	VIC	Melbourne	3000	Optus
197.***.***.***	98	EG	C	Cairo		TE Data

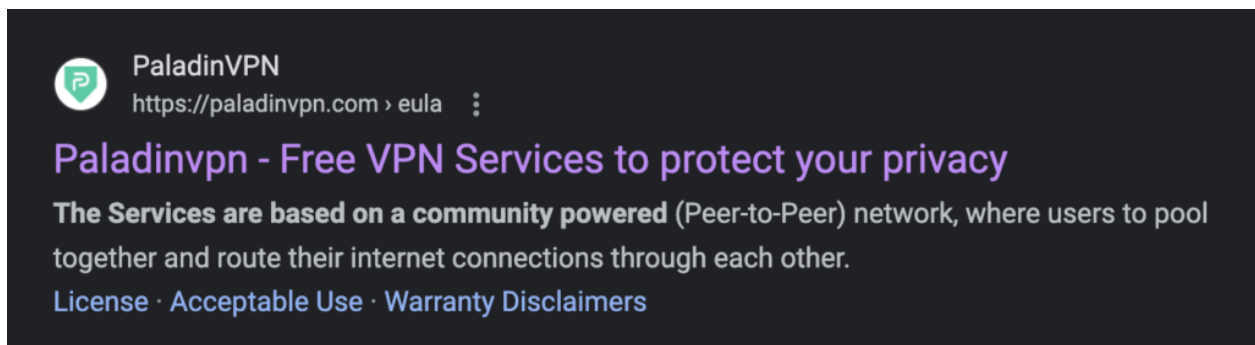
PortForwardList WhiteList Copy IP First Previous 1/3562 Next Last Refresh

Corporate needs you to find the difference between these two images

If the operators of 911 were lazy enough to reuse the same interface and backend (and I guess who can blame them), it's a safe bet that whatever app or apps are supplying their IPs are equally as obvious.

In the past, a key giveaway has been the verbiage in the free VPN apps marketing and/or EULA; these are usually just copy and pasted between all the clones. So that's probably a good place to start. Can we Google some phrases from MaskVPN's EULA and find anything obvious?

The Services are based on a community powered (Peer-to-Peer) network, where users to pool together and route their internet connections through each other. That means the software may make use of the Internet, among other means by re-routing some of your requests through other peer users. Your free use of the software will in turn enable other devices to be re-routed through your device. From that users can help each other to make the internet free for all, by sharing their idle resources. By using the Services you consent to the use of your device in the described manner and agree that other users or services may use your network connection and resources. You represent that your entry into this Agreement and your use of the Services does not breach any contract, duty, law, regulation or right, and that if sharing your resources is not desirable or allowed in your case, you will not use the Services, or purchase the MaskVPN enterprise version to use the network but not to contribute resources to it.



The screenshot shows the PaladinVPN website interface. At the top left is the PaladinVPN logo, a green circle with a white 'P'. To its right is the text 'PaladinVPN' and the URL 'https://paladinvpn.com › eula'. Below this is a purple heading: 'Paladinvpn - Free VPN Services to protect your privacy'. Underneath is a paragraph of text: 'The Services are based on a community powered (Peer-to-Peer) network, where users to pool together and route their internet connections through each other.' At the bottom of the screenshot are three links: 'License · Acceptable Use · Warranty Disclaimers'.

The EULA from MaskVPN vs. a quick Google search

Well that was easy. PaladinVPN is a “Free VPN” app, allowing users to route their traffic from their choice of 44(!) datacenter exits all over the world with no registration or payment required. But like the curling of a monkey's paw, there's always a catch.

Why is PaladinVPN free to use?

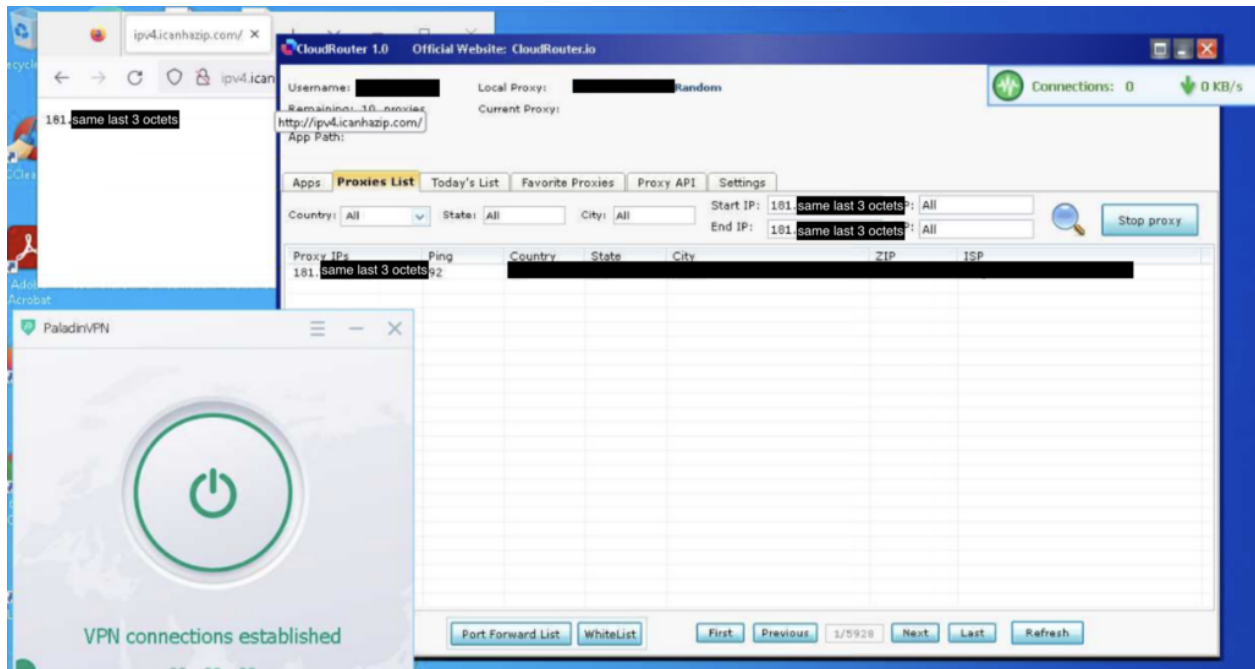
Why do cooperations and big institutions pay for your free VPN?

Big cooperations, brand holders, and institutions like banks or insurance companies are often misled or blocked when trying to access publicly available information on websites. The information displayed to them is often different from what a regular user sees. Our partners of PaladinVPN, collects data from the public websites for these cooperations and brand holders. In return, these companies pay for your free VPN by allowing Our partners to access the web via your IP address to gather the data. Below you find details and examples of data collected for these companies.

PaladinVPN explaining why it's free

I guess I have to give PaladinVPN *some* credit for, at the very least, warning their users that their IP is about to be co-opted by “companies” and “partners”. In any event, this a pretty good suspect in our search for the app that is (at least partially) feeding the IP pool for CloudRouter.

As it turns out, the easiest way to test this theory was to download and run PaladinVPN and see if we can buy our own IP on CloudRouter’s interface.



The smoking gun: IP search results in CloudRouter with PaladinVPN running in the background

And there it is. Upon firing up PaladinVPN, you are nearly immediately added to the list of purchasable IPs in CloudRouter’s interface. Our hunt was over as quickly as it started.

The lazy lie

Let’s read Paladin’s marketing a bit further. Maybe they elaborate on the shadowy entities who are about to use your IP address for who knows what.

What is our verification process for the use case?

Our partners has a very strict approval process to ensure only genuine and trustworthy companies and institutions are allowed access to the web via your IP address.

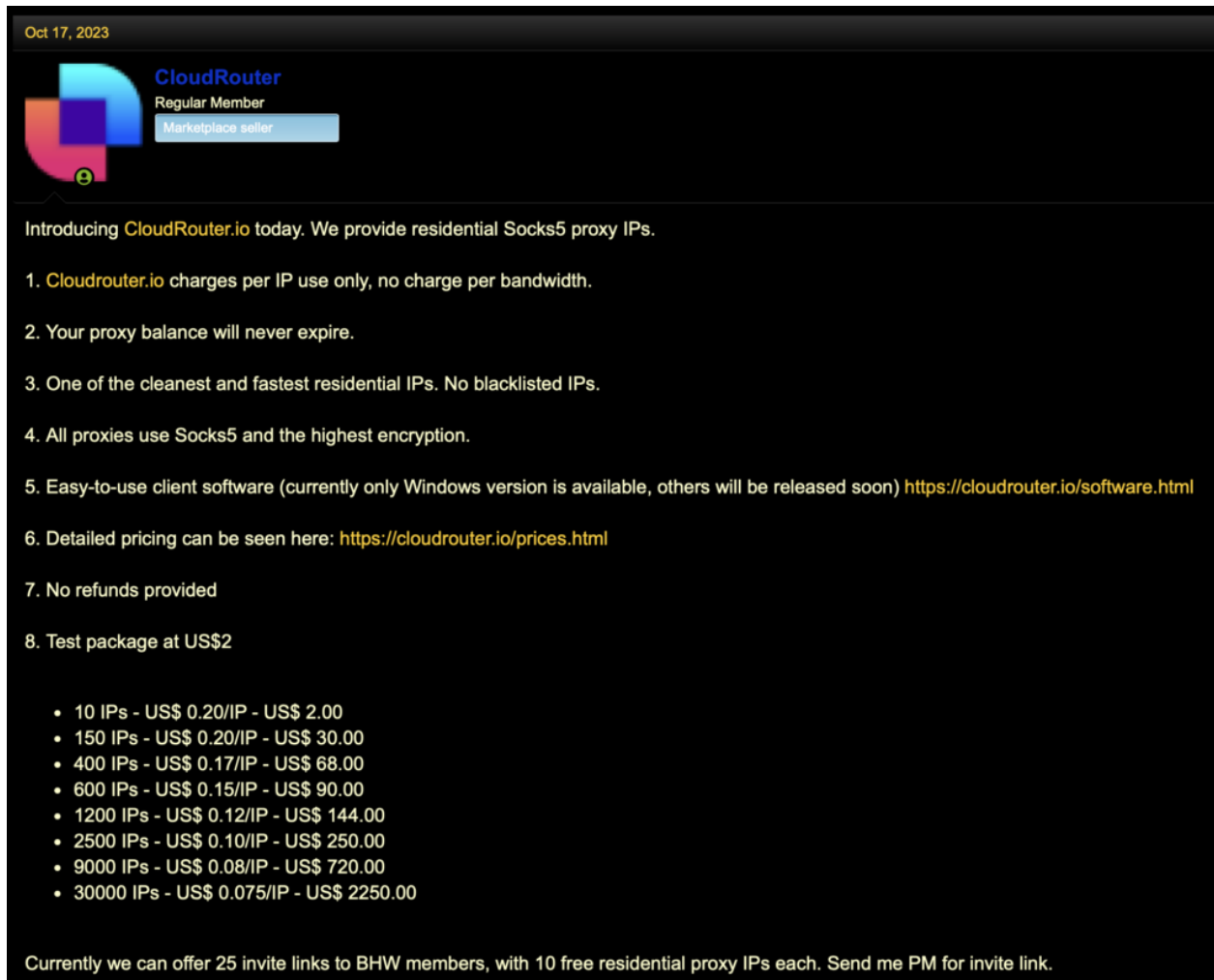
We do client verification and due diligence when onboarding new customers before they are allowed to use Our partners services. Our partners monitors the traffic in real-time to ensure that all traffic is within the TOS. Companies not complying with the strict rules will automatically be banned by our system.

We also provide 24x7 online support when you have any complaints. We do not tolerate illegal behavior like downloading illegal torrents!

[Download PaladinVPN →](#)

PaladinVPN KYC assurances

Some key phrases from their supposed KYC: “strict approval process”, “genuine and trustworthy companies and institutions”, “client verification and due diligence”.



Oct 17, 2023

CloudRouter
Regular Member
Marketplace seller

Introducing **CloudRouter.io** today. We provide residential Socks5 proxy IPs.

1. **Cloudrouter.io** charges per IP use only, no charge per bandwidth.
2. Your proxy balance will never expire.
3. One of the cleanest and fastest residential IPs. No blacklisted IPs.
4. All proxies use Socks5 and the highest encryption.
5. Easy-to-use client software (currently only Windows version is available, others will be released soon) <https://cloudrouter.io/software.html>
6. Detailed pricing can be seen here: <https://cloudrouter.io/prices.html>
7. No refunds provided
8. Test package at US\$2

- 10 IPs - US\$ 0.20/IP - US\$ 2.00
- 150 IPs - US\$ 0.20/IP - US\$ 30.00
- 400 IPs - US\$ 0.17/IP - US\$ 68.00
- 600 IPs - US\$ 0.15/IP - US\$ 90.00
- 1200 IPs - US\$ 0.12/IP - US\$ 144.00
- 2500 IPs - US\$ 0.10/IP - US\$ 250.00
- 9000 IPs - US\$ 0.08/IP - US\$ 720.00
- 30000 IPs - US\$ 0.075/IP - US\$ 2250.00

Currently we can offer 25 invite links to BHW members, with 10 free residential proxy IPs each. Send me PM for invite link.

CloudRouter advertisement on BlackHatWorld. Ooo, free samples!

Turns out their “strict approval process” ends at any script kiddie on BlackHatWorld with access to \$2 in Bitcoin.

Slaying the Hydra

We’d be remiss if we didn’t mention the IOCs for CloudRouter. The C2 servers are located at the IP addresses below; you’d see callouts on TCP port 500 to them from “compromised” devices.

98.126.169.2
67.229.56.2
67.198.222.194
67.198.221.50
67.198.221.250
67.198.221.226
67.198.221.194
67.198.221.186
67.198.212.2
174.139.10.82

At time of writing, we track all 44 PaladinVPN exit IPs and some ~140,000 CloudRouter IPs. It seems unlikely that the entirety of CloudRouter's pool is stemming from a single terrible free VPN application; we're not entirely sure where the rest are coming from. Frankly, of the ~22,000,000 residential proxy IPs we track, we likely couldn't give a concrete source for 80% of them. This is the true insidiousness of the residential proxy. They are ubiquitous, they are stealthy, and they are under-appreciated for the extreme risk of fraud and abuse they present.



PaladinVPN

A free VPN service that sells access to the VPN user's bandwidth, contributing to the pool for CloudRouter proxy

FREE_VPN

Protocols

PROPRIETARY

Free Tier



Allows free usage

45

Unique Active IPs

 26%

Avg Daily IP Churn

 18

Avg Devices/IP

 12

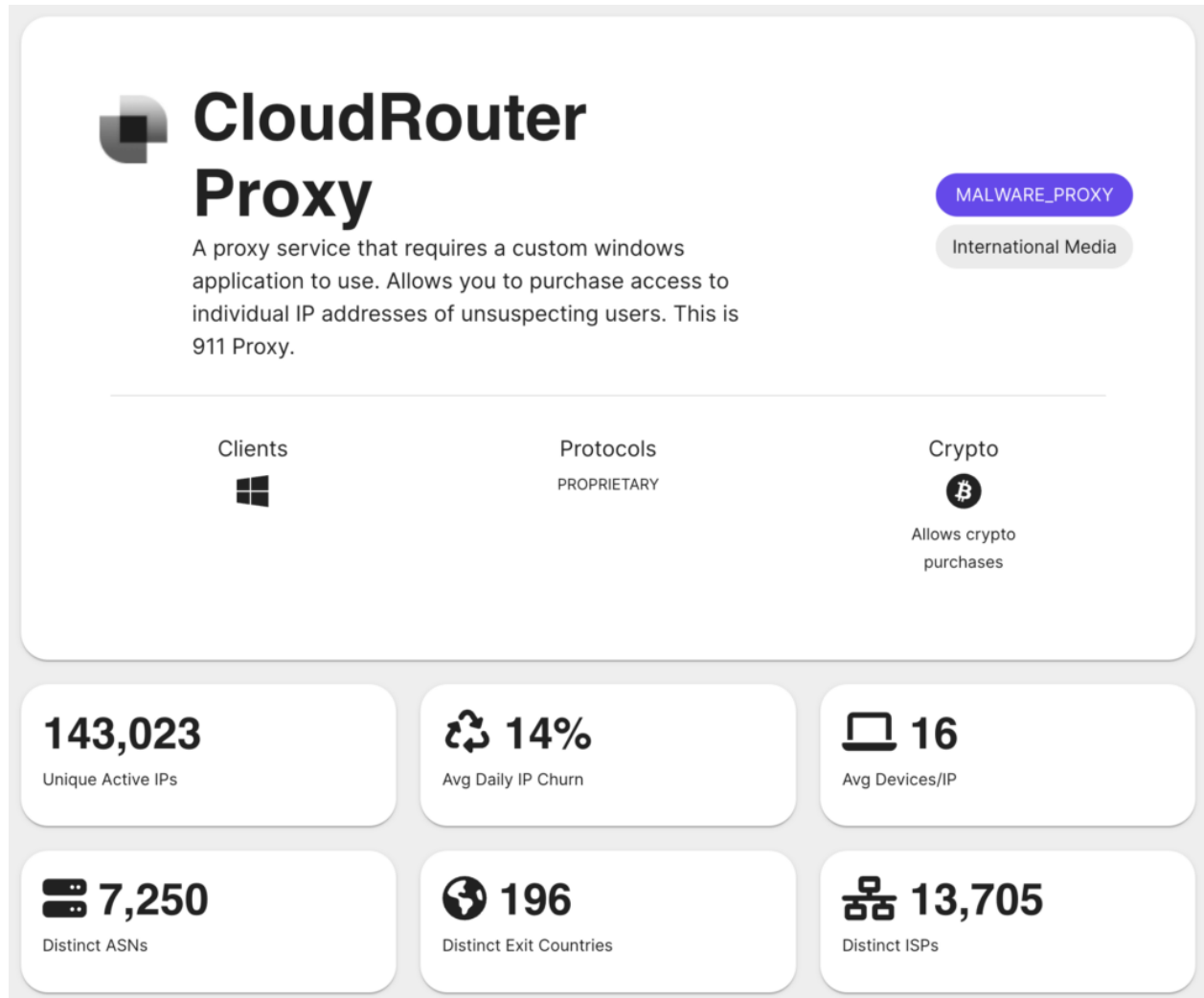
Distinct ASNs

 29

Distinct Exit Countries

 43

Distinct ISPs



Spur Dashboard results for PaladinVPN and CloudRouter

Monitoring malicious proxies such as 911.re and CloudRouter is an unending challenge. The lucrative nature of the residential proxy market ensures that as soon as one service goes dark, another inevitably takes its place, like The Hydra growing another head. Check out our [Community Dashboard](#) to get some insight into our extensive efforts in tracking these services.