# Characterizing Abusive IP Proxies

## A NETSEC Incident Response RFC

March 30, 2026

## Audience, Scope, and Purpose

This document is intended for network operators, security practitioners, policy authors, and abuse-response teams. Its goal is to establish shared terminology for discussing IP proxy technologies in the context of abuse detection, mitigation, and attribution.

## Introduction

The phrase “Internet proxies” can cover a variety of underlying technologies and objectives. This document covers terms and descriptions in an effort to avoid confusion when discussing abusive Internet Protocol (IP) proxy types and behaviors.

An IP Proxy could be defined this way:

> *An intermediary system, service, or application between two or more communicating endpoints. The endpoints communicate and terminate sessions at the IP layer through the intermediary rather than directly. This may be done for the purpose of endpoint protection, hiding, resource sharing, or gating between two otherwise unconnected networks. An IP proxy has access to communications above the IP layer.*
>
> *IP proxies may act transparently. Of particular concern are malicious proxies installed or configured without the knowledge of or explicit configuration by the system endpoint owner. Some specific uses of these proxies are control of the proxied connection and bypass of NATs or firewalls. Since each proxied endpoint communicates with a proxy IP address the actual remote endpoint is often indistinguishable from the proxy.*
>
> *There are a number of different protocol specifications that define intermediate communication between an endpoint and proxy. The client-side connection of a proxy may require the use of an authentication mechanism.*

IP proxies have been used for a variety of purposes, both legitimate and nefarious. As of this writing, there has been an explosion in the number of active IP proxies used for abuse. While proxies can and do serve legitimate purposes, abusive proxies are often installed on networks and devices without the explicit permission or the owner’s knowledge. Proxy functionality has also been concealed in other applications. IP proxies can hinder attribution of original attack sources, leading to responses that can harm unwitting proxy operator users and applications. Running an IP proxy and facilitating certain types of traffic may violate an ISP’s terms of service

(ToS)/acceptable usage policy (AUP) and subject the owner to various penalties including network restrictions, disconnection, fines, or legal risks. Malicious proxy operators often seek to leverage the reputation of the host system(s) or network(s) to mask the harmful activities and/or make the proxies more difficult to block without inflicting collateral damage. The malign network traffic can and often does cause reputational damage to the IP address(es) running the proxy which also impacts network operator reputation.

Other related intermediary devices may share challenges of attribution to an original source and can lack fine-grained policy controls. Examples include virtual private network (VPN), network address translation (NAT) and protocol translation relays.  Some intermediary devices may perform multiple functions, and the difference between intermediaries can be opaque.  Terms are sometimes used interchangeably or to highlight distinctions in primary function.

# IP Proxy Types / Categories with Examples

| Type | Description | Examples |
|---|---|---|
| App-embedded | Bundled into user-application software. Common in mobile apps and pre-compiled software packages. May offer system owners incentives for installation and operation. | Hola, Honeygain, Luminati / BrightData, Oxylabs |
| Commercial | Professionally developed and supported proxy software and infrastructure. | Zscaler, Securely, Netskope |
| Compromised | A system undermined with the installation of proxy capabilities for unauthorized use. | Routers with easily bypassed authentication protection and reconfigured to act as a proxy. |
| Data center | Dedicated hosting provider network proxy systems or networks. | Decodo, IPRoyal |
| Mobile | Proxies on or attached to cellular / mobile phone networks. | Bright Data, Limeproxies |
| Open | Public-use or publicly accessible proxy systems | Unprotected Squid proxies, 6to4 relays |
| Privacy | Anonymizing services designed to limit surveillance and traffic analysis. | Tor, iCloud Private Relay, Cloudflare WARP |
| Resnet | Networks or address blocks with proxies masquerading as residential networks. | ResNet |
| Residential | App-embedded proxies or compromised systems on residential networks and IoT appliances. | Mirai variants, SocksEscort |
| Reverse | Reverse proxies commonly provided by CDNs for content resiliency. | Cloudflare |

*Note: Proxies may belong to multiple of the above categories.*

Abusive IP proxies have been used to facilitate unwanted activity including, but not limited to:

- Denial of Service (DoS) or Distributed DoS attacks
- Spam
- Man-in-the-middle attacks
- Scanning, crawling, and scraping
- Click-fraud
- Intellectual property theft
- Bandwidth theft
- Infrastructure policy bypass
- Geolocation distortion
- Avoidance of server/service security measures

# References


- Koblas D. and Koblas, M.R, SOCKS, USENIX Security Symposium, 1992, https://www.usenix.org/conference/sec92/socks.
- Leech M., Ganis M., Lee Y., Kuris R., Koblas D., and Jones L, SOCKS Protocol Version 5, IETF RFC 1928, March, 1996, https://www.rfc-editor.org/rfc/rfc1928.
- Carpenter B. and Moore K., Connections of IPv6 Domains via IPv4 Clouds, IETF RFC 3056, February, 2001, https://www.rfc-editor.org/rfc/rfc3056.
- Weaver, N., Kreibich, C., Dam, M., and Paxson, V., Here Be Web Proxies. Passive and Active Measurement, 2014, https://doi.org/10.1007/978-3-319-04918-2_18.
- X. Mi et al., Resident Evil: Understanding Residential IP Proxy as a Dark Service, IEEE Symposium on Security and Privacy, 2019, https://doi.org/10.1109/SP.2019.00011.
- Krebs, B. The Rise of “Bulletproof” Residential Networks, April 19, 2019, https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks/.
- Mi, Xianghang, Tang, Siyuan, Li, Zhengyi, Liao, Xiaojing, Qian, Feng, and Wang, XiaoFeng. Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks, Network and Distributed System Security Symposium, 2021, https://doi.org/10.14722/ndss.2021.24008.
- Krebs, B., The Kimwolf Botnet is Stalking Your Local Network, January 2, 2026, https://krebsonsecurity.com/2026/01/the-kimwolf-botnet-is-stalking-your-local-network/.
- No Place Like Home Network: Disrupting the World’s Largest Residential Proxy Network, January 28, 2026, https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network.
- Squid, https://www.squid-cache.org, last accessed 2026-03-09.
- The Tor Project, https://torproject.org, last accessed 2026-03-09.
- Europol and international partners disrupt ‘SocksEscort’ proxy service, March 12, 2026, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-international-partners-disrupt-socksescort-proxy-service.

- Federal Bureau of Investigation, Evading Residential Proxy Networks: Protecting Your Devices from Becoming a Tool from Criminals, March 12, 2026, https://www.ic3.gov/PSA/2026/PSA260312.
- Authorities disrupt world's largest IoT DDoS botnets responsible for record breaking attacks targeting victims worldwide, March 19, 2026, https://www.justice.gov/usao-ak/pr/authorities-disrupt-worlds-largest-iot-ddos-botnets-responsible-record-breaking-attacks.
- Cloudflare, https://www.cloudflare.com, last accessed 2026-03-19.
- Cloudflare WARP, https://one.one.one.one, last accessed 2026-03-16.
- Decodo, https://decodo.com, last accessed 2026-03-19.
- Hola, https://hola.org, last accessed 2026-03-16.
- Honeygain, https://www.honeygain.com, last accessed 2026-03-17.
- iCloud Private Relay, https://support.apple.com/en-us/102602, last accessed 2026-03-16.
- IPRoyal, https://iproyal.com, last accessed 2026-03-19.
- Limeproxies, https://www.limeproxies.com, last accessed 2026-03-19.
- Luminati, https://brightdata.com/luminati, last accessed 2026-03-16.
- Mirai, https://en.wikipedia.org/wiki/Mirai_(malware), last accessed 2026-03-16.
- NETSEC, https://www.first.org/global/sigs/netsec/, last accessed 2026-03-16.
- Netskope, https://www.netskope.com last accessed 2026-03-16.
- Oxylabs, https://oxylabs.io, last accessed 2026-03-16.
- Request for Comments, https://en.wikipedia.org/wiki/Request_for_Comments, last accessed 2026-03-16.
- Securely, https://www.securly.com, last accessed 2026-03-16.
- Zscaler, https://www.zscaler.com, last accessed 2026-03-16.


## Acknowledgments


This document is a product of the FIRST NETSEC SIG. The following people contributed to this document: Paco Monserrat Coll, Rich Compton, Roland Dobbins, Serge Droz, Scott Fisher, Carlos Friaças, John Kristoff, Miles McCredie, Damian Menscher, Andreas Mühlemann, Phillippe Oesch, Tayfun Özaltin, Max Resing, and Tony Tauber.