rayobyte

TRANSPARENCY IN ACTION

RAYOBYTE'S PROACTIVE APPROACH TO INTERNET ABUSE PREVENTION

ayobyte

Content

Introduction

For too long, proxy providers have operated in the shadows, trying not to call too much attention to their business practices. Rayobyte is trying to do things differently. With the publication of this document, we hope to provide a full and transparent accounting of our three-pronged approach to fighting abuse - the first published by any provider in our industry.

For our customers, we hope reading this will give you confidence that you are working with an ethical company that takes these things seriously. For anyone whose sites are accessed by Rayobyte, you can have the utmost confidence that we are keeping your safety top of mind. For other proxy providers, new proxy providers and resellers, we hope you will adopt these practices yourself (or share better ones!) to take care of potential abuse on your network.

This whitepaper will cover:

- The challenge of internet resource abuse in the 2020s
- Rayobyte's three-pronged approach to fighting abuse
- How we detect, prevent, and respond to abuse concerns
- The difference between fighting abuse of data center and residential proxy resources

The Challenge of Internet Abuse

The Impossibility of Total Prevention

In the modern digital era, the Internet provides unparalleled opportunities for businesses and individuals to connect, discover, share, and exchange information. However, these opportunities naturally bring challenges that pose a threat to the intended good.

To a certain extent, the abuse of internet resources is inevitable. Giants like Google, Amazon, and Microsoft, with their extensive resources and advanced technologies, still encounter instances where their systems are manipulated or exploited:

- Google Cloud published a document in 2021 that showed their resources were being compromised by hackers and used to host malware, launch DDoS bots, send spam, and conduct large-scale cryptocurrency mining without device owners' awareness.
- Amazon Web Services (AWS) had an Elastic IP Transfer feature that made its IPs very easy to take control of and abuse for phishing, DDoS, and data theft, leading to some siteowners blocking AWS IP addresses entirely from their services.
- Microsoft's Remote Desktop Protocol (RDP) allowed hackers to augment the impact of Distributed Denial of Service (DDoS) attacks. By exploiting the vulnerabilities of RDP, attackers could enlist a large number of compromised systems to overwhelm specific targets, highlighting the evolving tactics used in cyber assaults.

These scenarios illustrate a critical truth in the digital landscape: it is impossible to completely eliminate the abuse of IP addresses and internet resources. This reality does not stem from a lack of effort or innovation but rather from the inherent, ever-evolving complexity of the internet and its users.

Technological efforts to prevent abuse have made great strides in the decade since Rayobyte's founding, but they will never be perfect. As Douglas Adams memorably wrote, "The major difference between a thing that might go wrong and a thing that cannot possibly go wrong is that when a thing that cannot possibly go wrong goes wrong, it usually turns out to be impossible to get at and repair.

We make this point not to exonerate proxy providers like ourselves of all responsibility. We understand that our role as a proxy IP address provider places us at a critical juncture in the fight against digital abuse. But our approach is rooted in the understanding that while the proxy industry has made significant strides in reducing the incidence and impact of internet abuse, prevention is only part of the solution.

The Three-Pronged Approach

Any comprehensive response to proxy abuse (or indeed, abuse of any kind of internet resource) needs to consist of three prongs: prevention, detection, and response.

- Prevention: we believe it is the responsibility of all proxy providers to implement measures to avert abuse before it occurs, such as stringent user verification, robust authentication processes, and educating users about responsible use.
- Detection: we believe it is the responsibility of all proxy providers to identify abuse when it happens, as quickly as possible. Any serious detection implementation requires a mixture of advanced automated monitoring tools and manual vigilance.
- Response: we believe it is the responsibility of all proxy providers to take swift and effective action against identified abuses. This includes enforcing strict penalties, collaborating with law enforcement and other relevant authorities, and continuously refining security protocols based on the nature of the abuse detected.

Our implementation of the three-pronged approach differs greatly when it comes to our data center and ISP proxy product line versus our residential and mobile product line. This is because data center proxies have a lower level of anonymity - it is easier to determine who is using a data center proxy and when and take action against a bad actor. Conversely, this is almost impossible to do with a residential proxy. This anonymity is the exact feature that makes residential IPs so appealing to our customer base, but it also means that we have a much greater responsibility to limit the sale and spread of these IP addresses.

Why Rayobyte Cares

To some readers of this document, the need for anti-abuse measures may seem self-evident. However, we are occasionally asked even by our legitimate customers why we go to the lengths we do to address abuse. As you will soon see, on the residential side of our business, we take our inspiration from the “Know Your Customer” process originated by banks worldwide, requiring a comparable level of information from our customers - an awful lot for a small IP address provider to ask of its clientele.

We will leave discussions of the legal responsibility of IP providers out of the scope of this whitepaper, as the legal landscape here is still in its infancy and varies greatly from country to country. Instead, we will discuss the practical and philosophical reasons why Rayobyte believes the processes outlined in this document are necessary and appropriate measures to take.

On the philosophical side, we consider proxies a tool. We have often used the analogy of a hammer. You can use a hammer for many wonderful and moral uses, like building a house for your children or constructing a temporary shelter for the homeless - and this is the most common function of a hammer. You can also use a hammer for violence, such as bashing a car window in. Likewise, proxies are mostly used for ethical uses, like powering the data analysis or search engine software that you and I use everyday. Without proxies and scraping, society as a whole would notice its impact:

- Google: A scraper at its core, Google utilizes the power of scraping to crawl the entirety of the internet to display the most relevant sites for our queries.
- Trivago: When purchasing a flight, hotel, and/or mode of transportation, Trivago aggregates information for you by scraping the web at scale to provide you with the best pricing options for your trip.
- Amazon: Known for its low prices and logistical genius, Amazon can price so competitively through the use of proxies and scraping of competitor sites.

This is merely a taste of the far-reaching effects proxies and web scraping have on our world today. Why then, require a KYC? The tool seller is not generally liable for what someone does with the tool they are sold. We don't require background checks for hammers. The distinction, for us, is that the damage that proxies can do is so much greater than violence against a single person. One need only consider the example of RSOCKS, a Russian proxy provider that was using its IPs to hack millions of devices worldwide on behalf of a major crime syndicate. Proxies can be - and have been - used to DDoS websites, hack into accounts via brute force, impersonate identities online, and more. We therefore see proxies as a tool that is still mostly used for good, but whose potential for harm is so great that it would be irresponsible to allow for its unchecked distribution.

Thus we see these measures as broadly necessary to ensure the safety of our customers, our business, our industry, and yes, the free and open internet as a whole. As we go through our anti-abuse measures in specific we will highlight the specific need for each one in turn as Rayobyte sees it.

ayobyte

Data Center

Data Center

PREVENTION

Static Proxies Have Low Appeal to Abusers

For reasons that will be explained in section 3.2 and 3.3, it is very easy to detect and ban anyone attempting an attack with data center or ISP proxies. Because criminals know this, they are less likely to use data center proxies for this purpose. This is actually why Rayobyte stayed a data center exclusive provider for so long - we were unwilling to implement residential proxies until we were sure that we could do so safely.

Moreover, our business model for data center proxies inherently discourages misuse. Modern websites are adept at banning suspicious data center IPs, rendering them ineffective for extended periods. At approximately $1 per IP per month for a static IP address, it becomes cost-prohibitive for nefarious actors to engage in significant illicit activities.

This pricing model, combined with the static nature of our IPs, makes this product line inherently less appealing for criminal activities.

Port Blocking

Since day one of our company, we have blocked all ports that allow for email sending with proxies. We know that proxies can be used to do mass email spam for purposes that range from “gray area” activities like cold emailing to outright fraud or phishing, so we simply do not allow any such use case.

We also block all other ports that are not used with the HTTP(S) or SOCKS protocol such as SSH ports, FTP ports, etc. We are here only to serve customers who need proxies to access websites without limitations - not to help bad actors hack into servers via SSH.

Rate Limiting

To further safeguard against abuse, we are in the process of implementing custom rate-limiting rules. These rules prevent any single customer from sending an excessively high number of requests in a short period.

DETECTION

Automated Detection

One thing we pride ourselves on at Rayobyte is our massive, proprietary monitoring system which promptly notifies our engineers of any minor and major issues that need attention. And because we own most of our data center infrastructure end-to-end, we have a significant amount of control over all aspects of our product.

Our monitoring system is used primarily to ensure continuous uptime for our customers, but it also allows us to trigger abuse alerts. For example: if we see a lot of non-HTTP 200 connections from a customer, we can assume they have DDoSed a website. In such a case, our system can rate-limit them immediately and alert an engineer to investigate.

Manual Detection

As described in 3.1, data center proxies are rarely used for abuse, and as described in 3.3 such abuse can be shut down instantaneously. Because of this, we devote most of our research and development of automated techniques efforts towards residential proxies, and rely mostly on manual detection for data center abuse.

The key difference between data center proxies and residential proxies is that residential proxies are associated with a residential ISP, like Comcast or Verizon, and with an anonymous residential device. Conversely, as the name implies, data center proxies are associated with a data center, and the internet service provider for such connections is listed as “Rayobyte.” It is therefore extremely easy for any site owner to reach out to us if they see suspicious activity.

We lease a large portion of our IPs from a variety of vendors, and each of them will send us a ticket or email notification when they are notified of abuse by a website. For those IPs which we own, site owners can send tickets directly to hostmaster@rayobyte.com.

All of these inboxes are monitored by our 24/7 engineering team who can respond promptly to all concerns.

We also automatically monitor various online blacklists (RBLs and SBLs) and if we see these online tools reporting abuse, we investigate it proactively.

Blazing SEO is the original name of our company, and when we rebranded in 2022 we issued a “doing business as” agreement rather than establishing a new legal entity. Thus, some data center proxies will still be listed as belonging to “Blazing SEO” in online database records. These complaints should still be sent to hostmaster@rayobyte.

RESPONSE

We will err on the side of caution and choose to assume the vast majority of said complaints are legitimate. Here is how we handle specific cases:

- If the complaint comes from a small or niche website, we promptly add them to the blacklist and ban the user(s) interacting with their site.
- If the complaint comes from a larger website that proxy users may have legitimate reasons to access (e.g. a large search engine) we suspend the user(s) interacting with said site promptly, but may not add the site to the blacklist unless there are repeated complaints.
- If the complaint comes from a government agency or law enforcement, it is promptly escalated to management. We save and backup all connection logs and pertinent customer details relating to the abuse, which we have built plugins to do as quickly as possible. We provide all this information to the agency in question and then take whatever actions they request.

This is the only circumstance in which we provide personally identifiable information about customers to any third party.

Our target response time to take action in response to an abuse complaint is within 1 business day. If a reporter feels a need is more urgent, they can contact us at support@rayobyte.com indicating the urgency and our support team will escalate it promptly.

ayobyte

Residential

Residential

PREVENTION

The Rayobyte Blacklist

Over our long tenure in the industry, we have developed a comprehensive blacklist containing over 800 domains which Rayobyte users cannot access through our proxies. The domains on this list include (but are not strictly limited to):

- Banking, credit card, and other financial institution websites - we consider these inherently inherently inappropriate for proxy use
- Any login URL or authentication server - when we see traffic to these sites, it usually represents a brute force login attempt rather than legitimate activity
- API URLs - Since APIs by their nature allow for rapid repeated queries without IP bans, the use of proxies generally indicates a user who is attempting to access they shouldn't be
- Direct access to the IP address of a domain or server - self-evidently suspicious
- Sites which have reported suspected abuse to us in the past or simply requested to be added to the list - this can be done here.

A version of this blacklist is also used for data center proxies, though many of the use cases above are non-accessible to these types of proxies in the first place.

Know Your Customer

All residential proxy users must complete a short trial and application process before we sell them residential IPs. The trial consists of 50 MB, which we feel is enough to test the product but not enough to implement any sort of malicious attack.

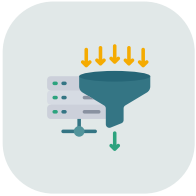
Following this, we require the user to go through a KYC ("Know Your Customer") process if any of the following is true:

- They access a site on our "graylist" of sites which are permitted but ripe for abuse
- They make what we consider a significant number of connections to the same website in a 24-hour period

- Their “risk score” - calculated based on account age, KYC status, and usage patterns - crosses a certain internal threshold

Our KYC requires the submission of detailed use case information as well as personal information (such as their passport) through the Sumsub platform, a highly secure and trusted platform used by the largest online businesses. We never export data from this platform - our customers’ personal information is always secure and out of our hands.

If the user refuses to complete a KYC, or if after doing so we find that the user cannot convincingly prove the validity of their use case, they are banned from the system.



Rate Limiting

As with data center proxies, we limit the numbers of requests per second that customers who have not completed a KYC can send. We also limit the number of requests to sites on the “graylist”.

We also limit usage based on certain other criteria that we believe may identify suspicious users. For example, if a user has a generic email address (e.g. one ending in “@gmail”), they are not allowed to connect to domains on the graylist unless they complete a KYC.

In short, we try to balance our customers’ desire for quick access to our residential proxy pool and the ability to “try before they buy” with the maximum in abuse prevention.

DETECTION

Real-Time Monitoring

The previous section described how we use both manual and automated monitoring to limit and detect potential abuse. Here are the specific things our system sends alerts for:

- Rate of requests per second
- Unauthorized access to “graylist” websites
- Behavioral fingerprinting to identify if a banned user may be returning under another account
- If a site has a significant number of non-HTTP 200 response codes in the past 15 minutes (this usually indicates a DDoS)
- Usage which does not match a user’s stated domains needed for their use case

Our system also monitors all “never before seen” domains with a significant number of connections in the past day. These domains are then subject to manual reviews by our engineering team and assigned a “risk score”. We are currently working on a tool which will use our in-house scraper API and generative AI to categorize domains automatically.

Manual Detection

All of the manual detection methods described in section 3.2 are utilized for residential proxies as well.

RESPONSE

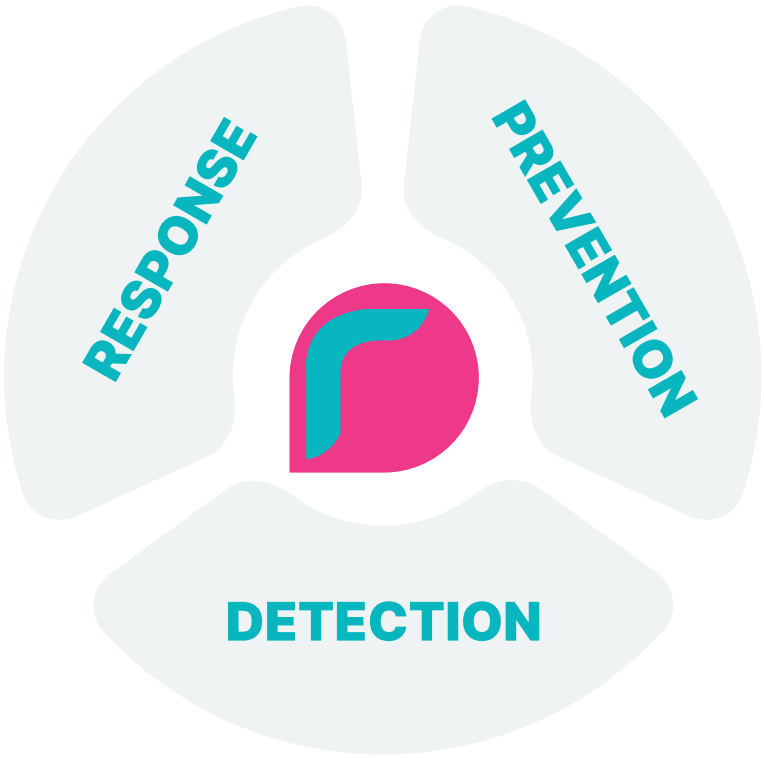
Unfortunately, responding to abuse complaints involving residential proxies is very difficult.

The process of abuse response usually looks like this:

- Site owner must contact law enforcement and informs them of the hack
- Law enforcement must subpoena the ISP
- The ISP gives the police the information they have about the residential customer who allowed us to use their IP address as a proxy.
- The residential customer doesn’t know how the hack happened and most law enforcement is “stuck” not knowing how to trace it more. Maybe they can look through all SDKs on a user’s device and contact each one, but that is very difficult to do and requires a significant number of resources.

Therefore, if abuse occurs and somehow makes it past our monitoring systems, due to the realities of how residential proxies work, it is very hard to detect, , let alone be able to find and ban the specific user who is doing it. This is why we invest so much in detection on the residential side. To our knowledge there has never been abuse of our residential product, and our #1 purpose as a company is to keep it that way.

Conclusion



The ultimate goal of our abuse processes is to directly combat those seeking to harm, and empower those seeking to do good through the use of the three-pronged approach: prevention, detection, and response. This approach ensures that proxy usage within our network prioritizes utmost care, security, and safety for all involved.

Whether you're a customer, a website owner, or a fellow proxy provider, we hope you feel encouraged to place your trust in Rayobyte's continually evolving and thorough abuse prevention processes. To our peers in the proxy community, we invite you to join forces with us in combating those who seek to undermine the integrity of proxies. By openly sharing and collaborating on abuse prevention practices, we can collectively make a positive impact and contribute to a safer online environment for everyone. Together, we have the power to effect change on a global scale.