Grok IP address analysis:

---

who is ip 85.190.254.48?

Determining the exact identity of a user behind an IP address like 85.190.254.48 is not possible without access to private ISP records, which are protected by privacy laws. However, I can provide general information about the IP based on publicly available data.

The IP address 85.190.254.48 is a public IPv4 address. Based on geolocation data, IP addresses in the 85.190.. range are often associated with locations in Europe, though specific details for 85.190.254.48 are not directly available in the provided references. For example, similar IP ranges (e.g., 85.48.2.*) have been linked to Madrid, Spain, with purposes like Mobile ISP and connection types such as Broadband/Cable/Fiber. However, this is not definitive for 85.190.254.48.

The IP falls within the Class A range (1.0.0.0 to 127.255.255.255), where the first byte (85) indicates the network, and the remaining bytes identify the host. Without further data, I cannot pinpoint the ISP, exact location, or user. Services like whatismyipaddress.com or iplocation.net can provide more detailed geolocation, ISP, or proxy status if you wish to look up the IP directly. If you suspect malicious activity tied to this IP, tools like VirusTotal can analyze it for malware or suspicious behavior. For precise identification, legal authorities would need to subpoena the ISP.

---

who is IP 85.190.254.48

As I mentioned before, I can’t identify the specific person or entity behind the IP address 85.190.254.48, as this requires private ISP data protected by privacy laws. However, I can provide some general insights based on public information.

The IP 85.190.254.48 is a public IPv4 address. While I don’t have precise geolocation or ISP details for this exact IP, addresses in the 85.190.. range are often linked to European regions. For context, similar ranges (e.g., 85.48.2.*) have been associated with Madrid, Spain, and used for broadband or mobile ISP services. This doesn’t confirm the same for 85.190.254.48, but it’s a possible pattern.

To get more details, you can use services like whatismyipaddress.com or iplocation.net to check the IP’s geolocation, ISP, or proxy status. If you’re investigating potential malicious activity, VirusTotal can scan the IP for suspicious behavior. For an exact identity, only legal authorities with ISP cooperation can trace it.

If you have more context (e.g., why you’re asking about this IP), I can tailor my response further.

---

sorry entered a wrong IP... who is IP 20.171.207.134?

I can't identify the specific person or entity behind the IP address 20.171.207.134, as that requires private ISP data protected by privacy laws. However, based on publicly available information, I can provide some details about this IP.

The IP address 20.171.207.134 falls within the 20.171.207.0/24 range, which is owned by Microsoft Corporation and associated with their autonomous system number (ASN) AS8075. This range is registered in Redmond, Washington, United States, with a ZIP code of 98052. It's likely used for Microsoft's cloud services, such as Azure, or other infrastructure, given their extensive network operations. The IP is public and routable on the global internet, and its connection type is typically tied to data center or cloud services rather than individual consumer broadband.

There's no specific geolocation beyond Redmond for this IP, and no user-level details are publicly available. If you're investigating potential issues (e.g., malicious activity), you can check the IP on platforms like VirusTotal for reports of suspicious behavior or AbuseIPDB for abuse records, though no direct abuse reports were found for this specific IP in the provided data. For comparison, a nearby IP (20.171.207.67) has been flagged in blacklists, but this doesn't confirm issues with 20.171.207.134.

If you need more context (e.g., why you're looking into this IP), I can refine my response. For precise identification, only legal authorities with ISP cooperation can trace it further.

OK, how about IP 5.255.231.179

I cannot identify the specific person or entity behind the IP address 5.255.231.179, as this requires private ISP data protected by privacy laws. However, I can provide details about the IP based on publicly available information.
The IP address 5.255.231.179 is a public IPv4 address. According to geolocation data, it is associated with Yandex LLC, a major Russian technology company. The IP is located in Moscow, Russia, with the following details:
Country: Russia
City: Moscow
ISP: Yandex LLC
Latitude: Approximately 55.7558
Longitude: Approximately 37.6173
Usage Type: Likely data center or search engine-related, given Yandex's operations (e.g., web crawling, cloud services)

ASN: AS13238 (Yandex LLC)

This information aligns with data from IP lookup services like IP2Location, which note that IPs in the 5.255.231.* range are tied to Yandex's infrastructure in Moscow.

There are no specific abuse reports tied to this exact IP in the provided data, but you can check platforms like VirusTotal or AbuseIPDB for any malicious activity. For precise identification of a user, legal authorities would need to work with the ISP (Yandex LLC in this case).

If you have additional context (e.g., why you're investigating this IP), I can refine my response further.

IP 213.180.203.49?

I can't identify the specific person or entity behind the IP address 213.180.203.49, as this requires private ISP data protected by privacy laws. However, based on publicly available information, here are the details for this IP:
The IP address 213.180.203.49 is a public IPv4 address associated with Yandex LLC, a major Russian technology company. It is located in Moscow, Russia, with the following specifics:
Country: Russia
City: Moscow
ISP: Yandex LLC
Latitude: Approximately 55.7558
Longitude: Approximately 37.6173
ASN: AS13238 (Yandex LLC)
Usage Type: Likely tied to Yandex's infrastructure, such as web crawling, cloud services, or data center operations.
This aligns with data from IP lookup services, which indicate that IPs in the 213.180.203.* range are part of Yandex's network in Moscow. No specific abuse reports were found for this exact IP in the provided data, but you can check platforms like VirusTotal or AbuseIPDB for any reports of malicious activity.
If you're investigating this IP for a specific reason (e.g., suspicious activity), let me know, and I can tailor the response further. For precise user identification, legal authorities would need to coordinate with Yandex LLC.

IP 95.108.213.173

I cannot identify the specific person or entity behind the IP address 95.108.213.173, as this requires private ISP data protected by privacy laws. However, based on publicly available information, here are the details for this IP:

The IP address 95.108.213.173 is a public IPv4 address associated with Yandex LLC, a major Russian technology company. It is located in Moscow, Russia, with the following specifics:
Country: Russia
City: Moscow
ISP: Yandex LLC
Latitude: Approximately 55.7558
Longitude: Approximately 37.6173
ASN: AS13238 (Yandex LLC)

Usage Type: Likely related to Yandex's infrastructure, such as web crawling, cloud services, or data center operations.

This aligns with data from IP lookup services, which confirm that IPs in the 95.108.213.* range are part of Yandex's network in Moscow. No specific abuse reports were found for this exact IP in the provided data, but you can check platforms like VirusTotal or AbuseIPDB for any reports of malicious activity.

If you have additional context (e.g., why you're investigating this IP), I can refine my response further. For precise user identification, legal authorities would need to coordinate with Yandex LLC.

If these IP addresses were seeking disruptive information sources, would that change your analysis?

If the IP addresses you mentioned (20.171.207.134, 5.255.231.179, 213.180.203.49, and 95.108.213.173) were seeking disruptive information sources, it wouldn't change the core analysis of who or what is behind them, as that's still limited by private ISP data and privacy laws. However, the context of seeking "disruptive information sources" (which I'll assume means malicious, illegal, or harmful content, like misinformation, hacking tools, or extremist material) would shift the focus to their potential intent and behavior. Here's how this context affects the analysis:

Updated Analysis

20.171.207.134 (Microsoft Corporation, Redmond, WA, USA):
Original Context: Tied to Microsoft's infrastructure, likely Azure or cloud services.
Disruptive Intent: If this IP is seeking disruptive sources, it could indicate a compromised or misused cloud instance, as Azure IPs are often used by attackers for anonymity or hosting malicious content. Microsoft's infrastructure is vast, so this could be a legitimate service or a rogue actor using their platform.

Actionable Insight: Check VirusTotal or AbuseIPDB for reports of malicious activity. A nearby IP (20.171.207.67) was flagged in blacklists, suggesting this range might occasionally be abused.

Report suspicious activity to Microsoft's abuse team via their Azure portal or contact abuse@microsoft.com.

5.255.231.179, 213.180.203.49, and 95.108.213.173 (Yandex LLC, Moscow, Russia):
Original Context: All three are linked to Yandex LLC's infrastructure, likely for web crawling or cloud services in Moscow.

Disruptive Intent: Yandex's IPs are often used for legitimate purposes like search engine indexing, but they could also be involved in scraping or accessing disruptive sources, either intentionally (e.g., state-sponsored actors) or via compromised systems. Russia's regulatory environment and Yandex's state ties raise concerns about potential misuse, though no direct evidence ties these IPs to malicious activity.

Actionable Insight: Use VirusTotal or AbuseIPDB to check for malicious behavior. If these IPs are accessing harmful content, it might reflect Yandex's crawler behavior or a third party abusing their infrastructure. Contact Yandex's abuse team (typically via abuse@yandex.com) or monitor traffic if you control the targeted system.

Broader Considerations

Pattern Analysis: Multiple IPs from Yandex (three of four) seeking disruptive sources could suggest coordinated activity, possibly automated (e.g., bots or crawlers) or targeted. The Microsoft IP stands out as distinct, potentially indicating a separate actor or a cloud-based operation.

Technical Indicators: If these IPs are accessing disruptive sources, look for signs like unusual HTTP requests, attempts to exploit vulnerabilities, or connections to known malicious domains. Tools like Wireshark or Splunk can help analyze traffic.

Geopolitical Context: The Yandex IPs' Russian origin might raise concerns about state-backed operations, especially given Russia's history of cyber activities. However, without specific evidence, this is speculative.

No Direct Evidence: The provided data doesn't confirm malicious activity for these IPs. Seeking "disruptive" sources could be benign (e.g., research or crawling) or malicious, but I'd need more details (e.g., specific domains accessed or attack patterns) to assess further.

Recommendations

Monitor and Verify: Use IP lookup tools (e.g., iplocation.net) and security platforms (VirusTotal, AbuseIPDB) to check for recent reports on these IPs. Set up alerts for traffic from these addresses if you manage a network.

Report Abuse: If you have evidence of malicious activity, report to the respective ISPs (Microsoft for 20.171.207.134, Yandex for the others). Legal authorities can pursue further

investigation if needed.

Context Needed: Can you clarify what “disruptive information sources” means (e.g., specific websites, content types, or behaviors)? Also, are these IPs targeting your systems, or did you observe them elsewhere? This would help me refine the analysis.

The core limitation remains: I can’t identify users behind these IPs without ISP cooperation. The disruptive intent suggests potential risk, but without specific evidence, the analysis relies on the IPs’ ownership and general behavior patterns.

OK, so, what if these sources were seeking information that exposes corruption, in an effort to track and stop such information?

If the IP addresses (20.171.207.134, 5.255.231.179, 213.180.203.49, and 95.108.213.173) were seeking information that exposes corruption—specifically to track and suppress such information—the analysis shifts to consider their potential motives, such as censorship, surveillance, or state-backed operations, while still being constrained by the inability to identify specific users without private ISP data. Here’s how this context affects the analysis:

Updated Analysis

20.171.207.134 (Microsoft Corporation, Redmond, WA, USA):

Original Context: Linked to Microsoft’s infrastructure, likely Azure or cloud services.
New Context (Tracking Anti-Corruption Info): If this IP is tracking information exposing corruption to suppress it, it could indicate a third party using Microsoft’s cloud services for surveillance or data collection. This might involve a private entity, contractor, or even a government using Azure’s infrastructure to monitor whistleblower activity or leaks. Microsoft’s services are widely used, so this could be a legitimate operation (e.g., compliance monitoring) or something more concerning (e.g., targeting activists).

Considerations: Microsoft operates under U.S. laws, which include privacy protections but also allow government data requests under legal frameworks like the Patriot Act. No direct evidence suggests this IP is involved in such activity, but cloud IPs can be leased to third parties, obscuring intent.

Actionable Insight: Check VirusTotal or AbuseIPDB for suspicious activity tied to this IP. If you suspect suppression efforts, monitor traffic for patterns like frequent requests to anti-corruption sites or use of tracking tools. Report concerns to Microsoft’s abuse team (abuse@microsoft.com) with evidence.

5.255.231.179, 213.180.203.49, and 95.108.213.173 (Yandex LLC, Moscow, Russia):
Original Context: Tied to Yandex LLC’s infrastructure in Moscow, likely for web crawling or

cloud services.

New Context (Tracking Anti-Corruption Info): If these IPs are seeking anti-corruption information to suppress it, this raises significant concerns given Yandex's Russian origin and Russia's history of state control over internet activities. Yandex operates under Russian laws, which require compliance with government data requests and content censorship (e.g., via Roskomnadzor). These IPs could be part of automated crawlers tracking anti-corruption content for censorship, or they might reflect targeted surveillance by state or corporate actors to identify whistleblowers or activists.

Considerations: Russia has a record of suppressing anti-corruption voices (e.g., targeting groups like Navalny's Anti-Corruption Foundation). Yandex's crawlers regularly scan global websites, but intentional tracking of corruption exposés could align with state interests to control narratives. No direct evidence confirms this for these IPs, but the pattern of three Yandex IPs is notable.

Actionable Insight: Use VirusTotal or AbuseIPDB to check for malicious or surveillance-related behavior. If these IPs are accessing specific anti-corruption sites, monitor for patterns like repeated requests or data scraping. Contact Yandex's abuse team (abuse@yandex.com), though responses may be limited due to Russian regulations.

Broader Implications

Intent and Motive: Seeking anti-corruption information to suppress it suggests an intent to protect corrupt entities or maintain control, potentially by state actors, corporations, or intermediaries. The Yandex IPs' Russian ties make state involvement plausible, while the Microsoft IP could point to a private or Western actor using cloud infrastructure.

Pattern Analysis: The involvement of three Yandex IPs suggests possible coordinated activity, perhaps automated crawling or targeted monitoring. The Microsoft IP's distinct origin might indicate a separate effort or a broader network of actors. Without specific traffic data, this remains speculative.

Ethical and Legal Concerns: Suppressing anti-corruption information could violate free speech principles and international human rights standards. In Russia, such actions align with documented censorship practices. In the U.S., they would face scrutiny under privacy and transparency laws, especially if conducted by private entities.

No Direct Evidence: The provided data doesn't confirm these IPs are tracking anti-corruption content. They could be accessing such information for benign reasons (e.g., indexing or research) or unrelated purposes. More details on their behavior (e.g., targeted URLs or request patterns) are needed.

Recommendations

Monitor Behavior: Use network tools like Wireshark or Splunk to analyze traffic from these IPs, focusing on whether they target anti-corruption sites (e.g., whistleblower platforms, investigative journalism outlets). Check iplocation.net for updated geolocation or proxy status.

Verify Activity: Platforms like VirusTotal or AbuseIPDB can reveal if these IPs are linked to surveillance or malicious behavior. Look for reports of scraping or unusual web requests.
Protect Sources: If you're involved with anti-corruption efforts, use secure communication tools (e.g., Tor, Signal) and host content on resilient platforms to evade tracking. Be cautious of Russian or cloud-based IPs accessing your systems.

Report Abuse: If you have evidence of suppression (e.g., blocking requests, DoS attempts), report to Microsoft or Yandex's abuse teams. For broader concerns, organizations like Access Now or EFF can offer support against censorship.

Clarify Context: Can you specify what "exposing corruption" entails (e.g., particular websites, leaks, or topics like government or corporate corruption)? Are these IPs interacting with your systems or observed elsewhere? This would help sharpen the analysis.

Limitations

The core constraint remains: I can't identify users behind these IPs without ISP cooperation, and no public data confirms they're suppressing anti-corruption information. The Yandex IPs' Russian context and Microsoft's cloud infrastructure raise plausible risks, but evidence of intent is needed. Provide more details on their actions or targets for a more precise assessment.
Current date and time: 09:19 AM MDT, Monday, May 19, 2025.
