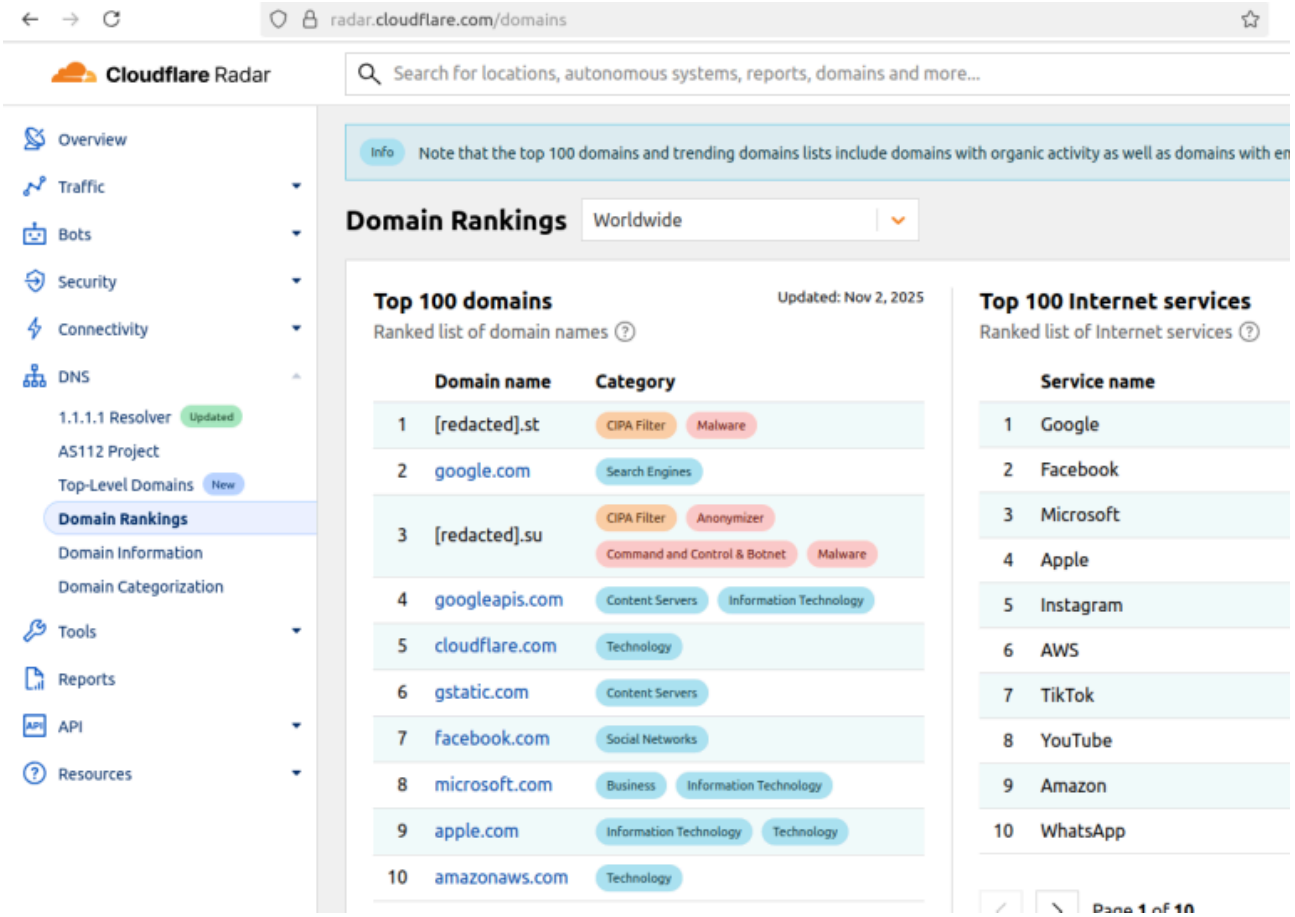
Cloudflare Scrubs Aisuru Botnet from Top Domains List

Published: 2025-11-06 · Archived: 2026-04-06 01:21:51 UTC

For the past week, domains associated with the massive **Aisuru** botnet have repeatedly usurped **Amazon**, **Apple**, **Google** and **Microsoft** in Cloudflare's public ranking of the most frequently requested websites. Cloudflare responded by redacting Aisuru domain names from their top websites list. The chief executive at Cloudflare says Aisuru's overlords are using the botnet to boost their malicious domain rankings, while simultaneously attacking the company's domain name system (DNS) service.



The #1 and #3 positions in this chart are Aisuru botnet controllers with their full domain names redacted. Source: radar.cloudflare.com.

Aisuru is a rapidly growing botnet comprising hundreds of thousands of hacked Internet of Things (IoT) devices, such as poorly secured Internet routers and security cameras. The botnet has increased in size and firepower significantly since its debut in 2024, demonstrating the ability to launch record distributed denial-of-service (DDoS) attacks nearing 30 terabits of data per second.

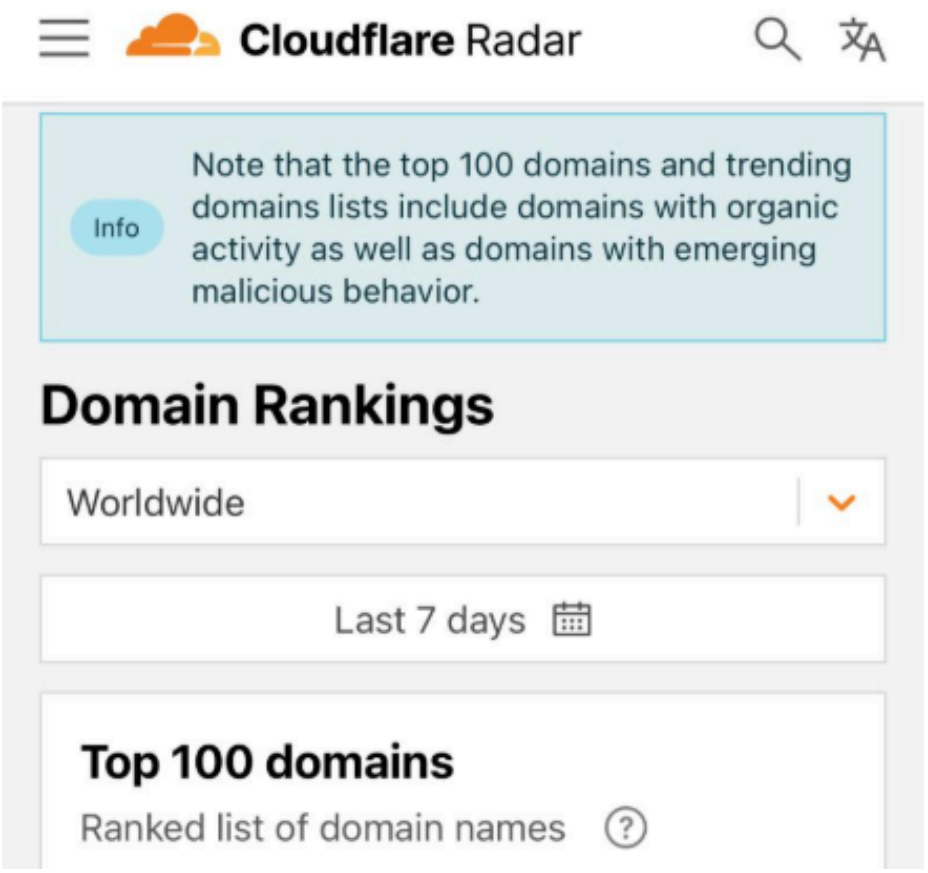
Until recently, Aisuru's malicious code instructed all infected systems to use DNS servers from Google — specifically, the servers at 8.8.8.8. But in early October, Aisuru switched to invoking Cloudflare's main DNS

server — 1.1.1.1 — and over the past week domains used by Aisuru to control infected systems started populating Cloudflare's top domain rankings.

As screenshots of Aisuru domains claiming two of the Top 10 positions ping-ponged across social media, many feared this was yet another sign that an already untamable botnet was running completely amok. One Aisuru botnet domain that sat prominently for days at #1 on the list was someone's street address in Massachusetts followed by ".com". Other Aisuru domains mimicked those belonging to major cloud providers.

Cloudflare tried to address these security, brand confusion and privacy concerns by partially redacting the malicious domains, and adding a warning at the top of its rankings:

"Note that the top 100 domains and trending domains lists include domains with organic activity as well as domains with emerging malicious behavior."



Cloudflare CEO **Matthew Prince** told KrebsOnSecurity the company's domain ranking system is fairly simplistic, and that it merely measures the volume of DNS queries to 1.1.1.1.

"The attacker is just generating a ton of requests, maybe to influence the ranking but also to attack our DNS service," Prince said, adding that Cloudflare has heard reports of other large public DNS services seeing similar uptick in attacks. "We're fixing the ranking to make it smarter. And, in the meantime, redacting any sites we classify as malware."

Renee Burton, vice president of threat intel at the DNS security firm **Infoblox**, said many people erroneously assumed that the skewed Cloudflare domain rankings meant there were more bot-infected devices than there were

regular devices querying sites like Google and Apple and Microsoft.

“Cloudflare’s documentation is clear — they know that when it comes to ranking domains you have to make choices on how to normalize things,” Burton wrote on **LinkedIn**. “There are many aspects that are simply out of your control. Why is it hard? Because reasons. TTL values, caching, prefetching, architecture, load balancing. Things that have shared control between the domain owner and everything in between.”

Alex Greenland is CEO of the anti-phishing and security firm **Epi**. Greenland said he understands the technical reason why Aisuru botnet domains are showing up in Cloudflare’s rankings (those rankings are based on DNS query volume, not actual web visits). But he said they’re still not meant to be there.

“It’s a failure on Cloudflare’s part, and reveals a compromise of the trust and integrity of their rankings,” he said.

Greenland said Cloudflare planned for its Domain Rankings to list the most popular domains as used by human users, and it was never meant to be a raw calculation of query frequency or traffic volume going through their 1.1.1.1 DNS resolver.

“They spelled out how their popularity algorithm is designed to reflect real human use and exclude automated traffic (they said they’re good at this),” Greenland wrote on LinkedIn. “So something has evidently gone wrong internally. We should have two rankings: one representing trust and real human use, and another derived from raw DNS volume.”

Why might it be a good idea to wholly separate malicious domains from the list? Greenland notes that Cloudflare Domain Rankings see widespread use for trust and safety determination, by browsers, DNS resolvers, safe browsing APIs and things like TRANCO.

“TRANCO is a respected open source list of the top million domains, and Cloudflare Radar is one of their five data providers,” he continued. “So there can be serious knock-on effects when a malicious domain features in Cloudflare’s top 10/100/1000/million. To many people and systems, the top 10 and 100 are naively considered safe and trusted, even though algorithmically-defined top-N lists will always be somewhat crude.”

Over this past week, Cloudflare started redacting portions of the malicious Aisuru domains from its Top Domains list, leaving only their domain suffix visible. Sometime in the past 24 hours, Cloudflare appears to have begun hiding the malicious Aisuru domains entirely from the web version of that list. However, downloading a spreadsheet of the current Top 200 domains from Cloudflare Radar shows an Aisuru domain still at the very top.

According to Cloudflare’s website, the majority of DNS queries to the top Aisuru domains — nearly 52 percent — originated from the United States. This tracks with my reporting from early October, which found Aisuru was drawing most of its firepower from IoT devices hosted on U.S. Internet providers like **AT&T**, **Comcast** and **Verizon**.

Experts tracking Aisuru say the botnet relies on well more than a hundred control servers, and that for the moment at least most of those domains are registered in the .su top-level domain (TLD). Dot-su is the TLD assigned to the former Soviet Union (.su’s Wikipedia page says the TLD was created just 15 months before the fall of the Berlin wall).

A Cloudflare blog post from October 27 found that .su had the highest “DNS magnitude” of any TLD, referring to a metric estimating the popularity of a TLD based on the number of unique networks querying Cloudflare’s 1.1.1.1 resolver. The report concluded that the top .su hostnames were associated with a popular online world-building game, and that more than half of the queries for that TLD came from the United States, Brazil and Germany [it’s worth noting that servers for the world-building game **Minecraft** were some of Aisuru’s most frequent targets].

A simple and crude way to detect Aisuru bot activity on a network may be to set an alert on any systems attempting to contact domains ending in .su. This TLD is frequently abused for cybercrime and by cybercrime forums and services, and blocking access to it entirely is unlikely to raise any legitimate complaints.
