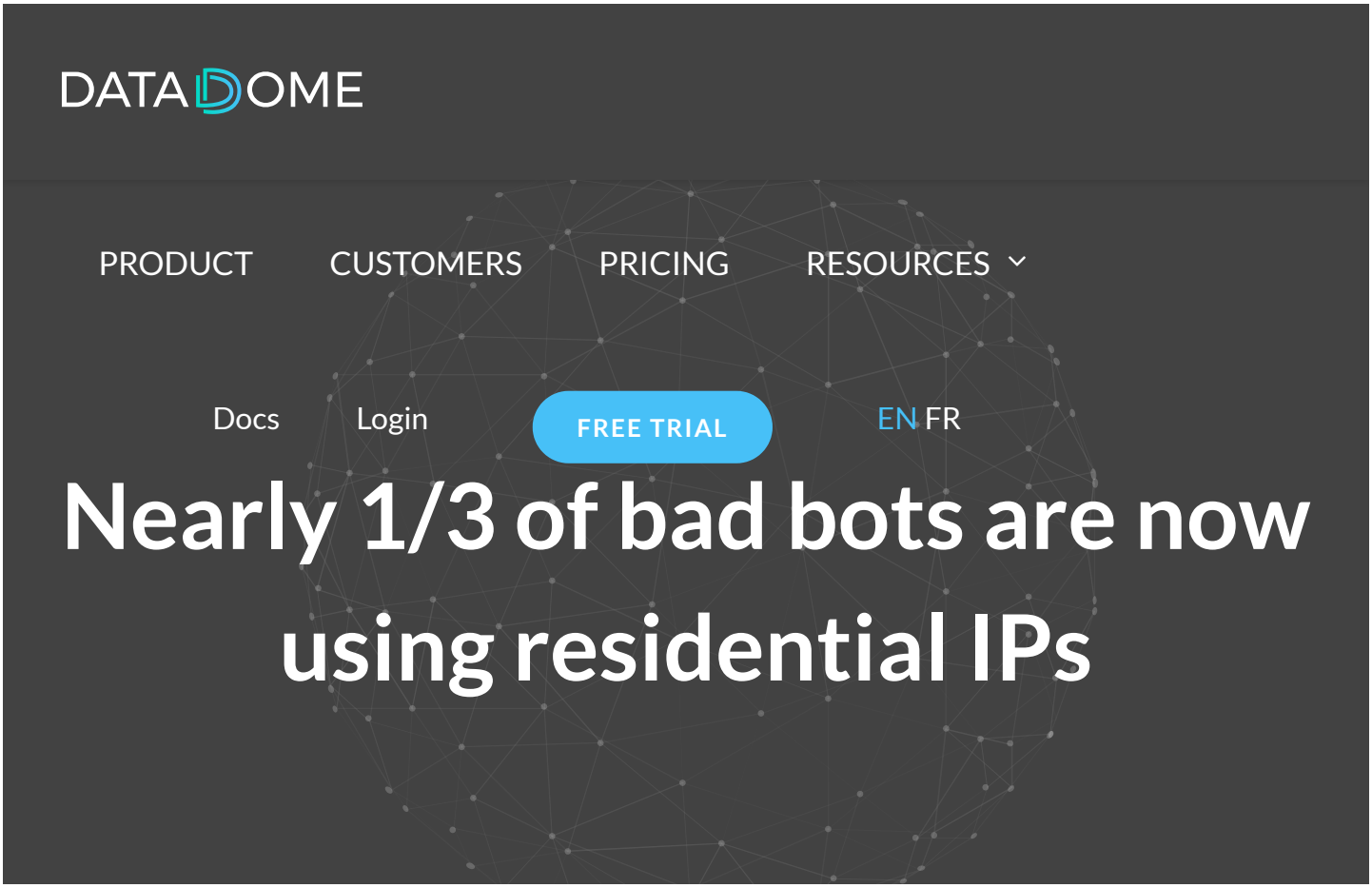


Detecting bad bots is a never-ending cat-and-mouse game, as bot operators continuously look for new ways to bypass bot detection systems.

While the first-generation bots of yesteryear were using different technologies than humans and were therefore reasonably easy to detect, today's bad bot traffic is almost indistinguishable from legitimate human traffic.

Rudimentary bots that couldn't execute JavaScript have been replaced by sophisticated programs that leverage advanced headless browsers, such as Headless Chrome. Bots also actively lie about their fingerprint to avoid detection.

But browser technologies and fingerprints aren't the only things bots operators have changed. In the race to bypass detection systems, they are also moving away from data center IP addresses that make them too easy to identify.

To blend even more seamlessly in with human traffic, **bad bots increasingly use residential IP addresses** instead of data center IPs. But *how* prevalent is this p[illegible]e

DATADOME

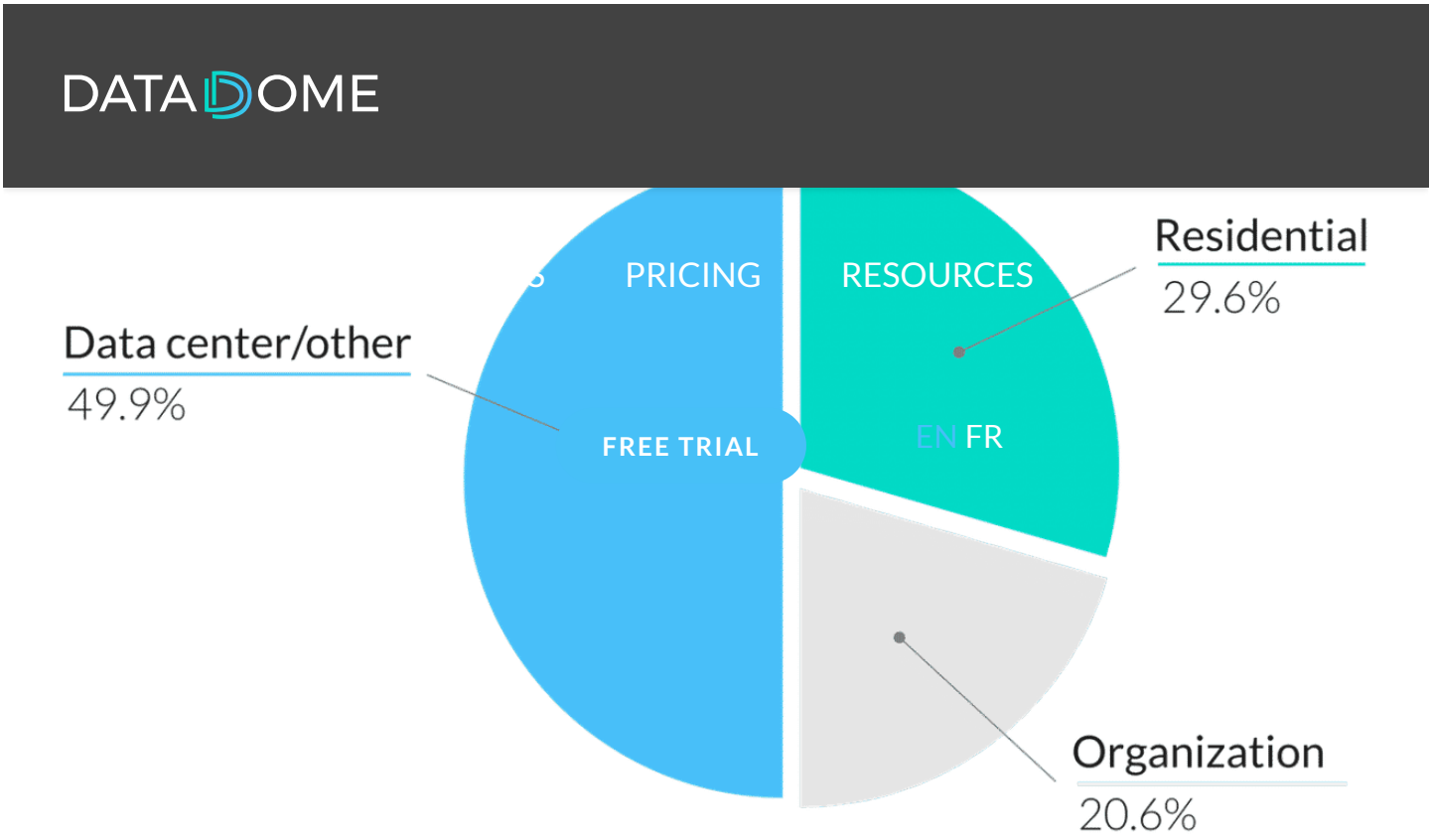
Residential IPs represented nearly 30% of bot req

As more and more websites and applications are setting up some form of protection against malicious automated traffic, bot developers are turning to residential IPs to camouflage their bots as legitimate traffic.

While residential IP addresses are more expensive than data center IPs, due to a more limited supply, they can be obtained easily enough through companies such as Geosurf or Luminati that provide **residential IP proxies**.

Out of the billions of bad bot requests we registered during the 2019 end-of-year holiday period, **29.55% were using a residential IP address**. This means that nearly **one in three** bad bots requests would pass for human traffic if you were looking at the IP address only.

We also found that **20.55% of bad bots came from an organizational IP address**. For the most part, these are probably infected devices that are exploited unbeknownst to the IP address owner. Poorly secured IoT devices, for example, are very popular among bad bot operators.



The takeaway: Security solutions that rely heavily on IP reputation are no longer a match for bad bot operators.

Bad bots that use residential IPs also lie about their nature

So if blocking unwanted traffic based on IP reputation is no longer a viable strategy, how about blacklisting bad user agents? Sadly, this isn't enough to protect your applications either.

Bot developers that go to the trouble of paying for residential IPs proxies are careful and motivated, and will often modify the user agent as well as the HTTP headers sent by their bots to remain under the radar.

Among the top 5 most common user agents used by bots, none belongs to known bots such as Headless Chrome or PhantomJS:

1. Mozilla/5.0 **(malformed user-agent)**

like Gecko) Chrome/78.0.3904.108 Safari/537.36 **(Chrome 78 on Windows 10)**

4. Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3[illegible]537.36 **(Chrome 79 on Windows 10)**
5. Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0 **(Firefox 67 on Windows 7)**

Except the first user agent on the list, which is malformed (it was used in a Layer 7 DDoS attack against one of our customers' websites), all the most common user agents that were used by the residential IP bots we detected are typical of human users.

The takeaway: Don't trust the user-agents your visitors declare, and don't base your anti-bot strategy on user agent blacklisting.

Bad bots that use residential IPs target mobile applications

Our original top 5 list included two mobile application user agents, but since these user agents make it easy to identify the targeted application, we removed them from the ranking.

However, the fact that two of the top five bot user agents were going after mobile applications highlights another shift in the way bots are acting: mobile API endpoints are increasingly being targeted.

Because most companies that have implemented anti-bot solutions focus primarily on protecting their website APIs, bot operators have turned to mobile app APIs.

to the mobile application APIs without being detected.

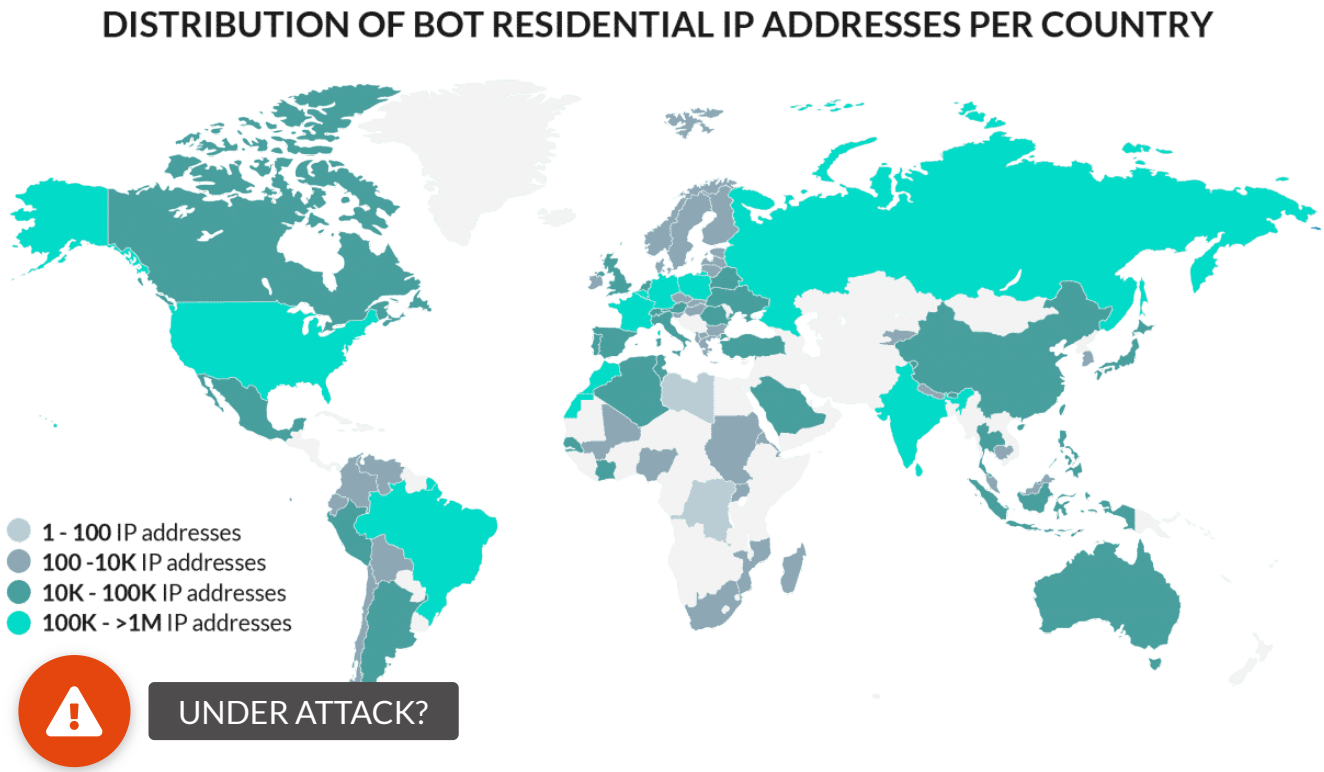
The takeaway: Anti-bot protection is just as important on your mobile application API as on your website API.

> **Learn more**: API security: How to protect mobile apps from bad bots

Bad bots use residential IPs worldwide

Next, let's take a look at the geographic distribution of bots that exploit residential IP addresses worldwide.

The map below shows the origin of the residential IP addresses used by the bots we detected during the holiday period.



Whenever we activate our bot protection solution on a website or application in a new country, we observe bad bot traffic routed through residential IP addresses in that country.

We also observe that bots tend to use residential IPs with the **same geographic origin as the target**, not as their own country of origin. Bots that want to scrape content from American websites will use American residential IP addresses; bots that conduct credential stuffing attacks against Australian websites use Australian residential IP addresses.

The takeaway: Blacklisting traffic from countries where you do not operate is ineffective. Not only do you run the risk of blocking legitimate users who are simply traveling or using a VPN for one reason or another; this strategy also leaves you unprotected against attacks conducted via infected residential IP addresses from your home country.

Residential IP addresses used by bots often have multiple targets

The residential IPs that are used by bad bots are often provided as part of proxy services or bot-as-a-service solutions, which means that they typically have multiple users that are targeting a range of different websites and applications.

During the two-week period we are analyzing here, we detected more than 1.2 million residential IP addresses used by bad bots that made requests to two or more websites or applications. Of these, there were **more than 105,000 IP addresses** that attacked **five or more different targets**.

3	257856	448483
4	84683	190627
5	41775	105944
6+	169	64169

While the bad bots that leverage residential IP addresses are often used for scraping purposes, it is not the only use case. Our data set includes **more than 100 million credential stuffing attempts** from these IPs, both on websites and mobile applications.

The takeaway: Bot attacks are no longer conducted by script kiddies and other amateurs. Today's bad bots are the products of a flourishing industry with considerable human, financial and technical resources at its disposal, and efficient protection must take that into account.

Efficient bot protection requires behavioral detection

To recap: Bad bots are using more and more sophisticated methods to bypass bot detection systems. They use real browsers or headless browsers with modified fingerprints, lie about their user agent, and increasingly rely on residential IP addresses located in the same country as their target to blend in with the humans. As much as a third of all bad bot requests now come from residential IP addresses.

As a consequence, security strategies that used to work—rate limiting, user agent blacklisting, or blocking traffic from foreign countries—are not effective anymore. W t ection knowledge, it is well-nigh impossible to ef ntly protect your applications against such advanced bots.

learning.

Known bots are detected via server-side fingerprinting in less than 2 milliseconds. The real challenge is new threats, which are identified via statistical and especially behavioral detection, using data e fingerprints, a JS rendering engine, SDK inputs and session tracking.

DataDome is used by high-profile websites worldwide, which benefits all our customers: whenever a new bot is detected on one of the more than 10,000 domains we protect, our algorithm updates itself so that all our customers are automatically protected against the new threat in less than 50 milliseconds. Data from an attack we detect on a German website, for instance, will help protect an American mobile application against the same threat.

Ready to try? Start your free trial today (it takes 10 minutes and you don't need a credit card), or contact us to request a demo.