

The background of the entire page is an abstract painting with thick, expressive brushstrokes. The color palette is dominated by dark blues, teals, oranges, and yellows, creating a sense of depth and movement. The composition is vertical, with a central white and yellow area that seems to recede into the distance.

# Initial Access Brokers, Russian Hacking Forums, and the Underground Corporate Access Economy

A detailed Analysis of 90 Days of IAB Activity on the Dark Web Forum Exploit

Eric Clay, Security Researcher



# Table of Contents

Introduction	3
Executive Summary	4
Initial Access Brokers as a Key Linchpin of the Cybercrime Ecosystem	5
The Anatomy of an IAB Post	6
Research Questions & Hypothesis	7
The Blitz, Auctioning Process, and Whale Hunting	8
How Many Threat Actors were Active During the Period?	11
U.S. Critical Infrastructure, IABs, and Types of Access	15
IABs and Russian Hacking Forums - An Urgent Call to Action	17



# Introduction

More than 100 companies across 18 industries had access to their IT infrastructure, cloud environments, networks, or applications sold on Russian hacking forums so far in 2023. Initial access brokers (IABs) operate across multiple dark web forums and specialize in gaining access to corporate IT environments which are then auctioned off or sold on dark web forums.

These actors are often sophisticated, focused, and specialized in finding vectors that can provide them access to corporate environments. In many cases they are also stunningly successful in gaining access to highly sensitive IT infrastructure, even for large sophisticated companies.

For this analysis Flare reviewed three months of initial access broker posts on the Russian hacking forum Exploit, in that time period we observed threat actors selling access to U.S. defense contractors, telecommunications companies, chemical manufacturers, energy companies, and companies across multiple more than a dozen other industries.

We collected, standardized and normalized 72 initial access auctions from May, June, and July to better understand how initial access brokers operate, who they target, how much they sell access for, and how active certain brokers are.



# Executive Summary

- Access to U.S. Critical Infrastructure (as defined by CISA) including Defense Contractors, Food Supply, Telecommunications, and Government Contractors was auctioned off on Russian hacking forums between May 1st and July 27th 2023.
- Attacks against U.S. companies were the most common, with 36% of all listings during the period advertising access to victims located in the United States.
- The top 7 threat actors studied were responsible for 55% of listings, indicating that a few threat actors active on the darkweb forum Exploit are responsible for the majority of posts.
- Finance and Retail were the most targeted industries during this period followed by Construction and Manufacturing.
- The average price of corporate IT access on Exploit during the time period studied with outliers removed is \$1,328. Prices ranged from \$150 to more than \$120,000 based on the type of access being sold, the country, and the industry of the victim.
- Access to RDP and VPN accounts accounted for the vector in 60% of all initial access broker posts.
- Some actors specifically advertised the lack of backup systems at victim companies, or advertised that they had access to backup systems. This suggests that some IABs likely expect the access they sell to be used for ransomware attacks.
- Based on posts from active initial access brokers, Flare analysts believe that it is highly likely that many initial access brokers are sourcing access from stealer logs found on Russian Market, Genesis Market, and public or private Telegram channels.



# Initial Access Brokers as a Key Linchpin of the Cybercrime Ecosystem

The cybercrime economy continues to grow. Threat actors now operate across thousands of Telegram channels, more than 100 Tor forums and marketplaces, and on numerous social media and encrypted messaging platforms. The majority of cybercrime activity is focused on consumer fraud; breaking into bank accounts, stealing cryptocurrency, and other criminal activity targeted at individuals. Only a small group of more sophisticated actors are known for targeting companies.

Cybercrime threat actors targeting corporate environments or that enable targeting that affects corporations generally fall under one of the following classifications:

**Stealer Log Vendors:** Many threat actors distribute stealer logs across Russian Market, Genesis Market, and public/private Telegram channels. In some cases as part of normal distribution threat actors inadvertently infect computers with credentials that include access to corporate access. This is likely a key source for initial access to RDP/VPN credentials that can be leveraged by IABs to establish and expand access.

**Hacktivist Groups:** There are numerous hacktivists that operate across Tor and Telegram including recently created groups such as Killnet and Anonymous Sudan that focus on attacking NATO countries' critical infrastructure and government agencies. These groups are often found in large, public Telegram channels.

**Ransomware Gangs:** Ransomware gangs often produce specific ransomware variants which they distribute themselves, or provide to affiliates who carry out attacks and take part in the profits. Ransomware gangs are increasingly leaking data as part of double and triple extortion schemes, in some cases ransomware groups are no longer even bothering to encrypt files. There are strong indicators that there is a direct link between initial access brokers and ransomware attacks.

**Initial Access Brokers:** These threat actors are primarily active on Russian hacking forums XSS and Exploit, they specialize in gaining initial access to IT environments which they then resale, likely to ransomware gangs, affiliates, nation states, and even other IABs.

This report is focused on initial access brokers. All posts were collected from the dark web forum Exploit and examined by analysts. We focused on extracting valuable features from each post that could be used to compare and contrast data.



The screenshot shows a Telegram post with a profile picture of a globe. The post details include: 'Paid registration', '29 posts', 'Joined 03/21/23 (ID: 107859)', and 'Activity хакинг / hacking'. The post content is: 'USA', 'Type: Rdp access', 'Aerospace & Defense', 'Windows 2008\AV: Defender, 31+ scan pc.', 'Local admin.', and 'Only sale through a guarantor exploit.'. Pricing information at the bottom reads: 'Start: 800\$', 'Step: 200\$', 'Blitz: 2000\$', and '12 hour/last bid'. A caption below the post reads: 'Post advertising RPD access for a U.S.-based aerospace & defense organization'.




# The Anatomy of an IAB Post

Understanding IAB posts isn't always simple. IAB posts are often a mix between English and Russian, with some exclusively written in Russian. There is also specific terminology that access brokers use that may not be familiar to the average English speaker.

- **Type/Тип доступа:** Describes the type of access obtained, most commonly RDP or VPN access.
- **Industry/Деятельность:** Describes the industry of the victim company. Finance, Retail, and Manufacturing are the three most common targets.
- **Access Level/Права:** Describes the level of privileges obtained.
- **Revenue:** Describes the revenue of the victim company, often obtained from U.S. based data providers publicly available online.
- **Host Online:** Often describes the number of hosts from the victim and sometimes includes antivirus and security systems in place.
- **Start:** The starting price of the auction.
- **Step:** The bid increments.
- **Blitz:** The buy it now price.

Тебе сказали... чудес не бывает? Не верь! Они их просто не видели...

●●●●



User  
+14  
178 posts  
Joined  
10/03/17 (ID: 83578)  
Activity  
хакинг / hacking

Доступ к фирме!  
GEO: USA  
Деятельность: Риелторы  
Revenue - \$5M  
Тип доступа: RDP Access  
Права: Domain Admin  
Host online: 47/ AV - Win Def, Cyber Protect  
Star: 400\$  
Step: 100\$  
Blitz: 1000\$  
PPS: 1 час! Последняя ставка!

---

Post advertising RPD access for a U.S.-based organization

While many posts contain all of this data, there is substantial variance between posts. Individual threat actors often have their own format for posts which may omit certain types of data. In addition, some threat actors deliberately left out data and asked potential purchasers to message them on Telegram for more information, likely in an effort to prevent law enforcement, threat intelligence providers and other organizations from determining the identity of the target.



# Research Questions & Hypothesis

We set out to answer the following research questions:

- What is the average “blitz” price that a threat actor sells corporate access for with outliers removed?
- Which countries are most represented in IAB posts?
- Do threat actors target specific industries more than others?
- How frequently is IT infrastructure access to organizations that are classified as U.S. Critical Infrastructure by CISA being sold?
- Do certain types of access fetch a higher price than others?
- What are the most common types of access that threat actors obtain and sell?
- How many threat actors exist in the ecosystem on Exploit? How much activity are the top actors responsible for?

We hypothesize that U.S. companies would be the most targeted in the world, and that access to U.S. organizations would sell for more than access to companies in other countries. In addition we expect that the IAB ecosystem on Exploit would be varied, with many threat actors providing individual listings.

## Research Limitations

- We only reviewed data from May 1st to July 27th, 2023 providing us a sample size of 72 IAB events. While this sample size was sufficient to provide interesting data, it limits some statistical analysis.
- Posts varied in information based on the threat actor. Key data such as industry, level of access, type of access and other key elements were missing from a small number of listings in our sample. In these cases data was listed as “unknown” for the analysis.
- We only reviewed IABs active on one dark web forum out of several forums where access brokers are active. Data discussed in this paper only focuses on the dark web forum Exploit.



# The Blitz, Auctioning Access, and Whale Hunting

We began our analysis by looking at the average “buy it now” or “blitz” for an initial access auction. The average price to purchase initial access across all samples in our data set was \$4,699.31, while with outliers removed it was \$1,328.23. This largely reflects the extreme range of listings present in the data set. Listings were as cheap as \$150 and could go up to more than \$120,000 for unique access to certain IT environments in high-value segments.

Distribution of IAB Blitz Prices



Distribution of blitz prices across our data set, excluding one extreme outlier

The histogram represents the distribution of blitz prices across our data set and excludes the single auction with a blitz price of \$120,000. It immediately stands out that the vast majority of listings are available for relatively low cost, with roughly a third of all auctions having a blitz price below \$1,000.

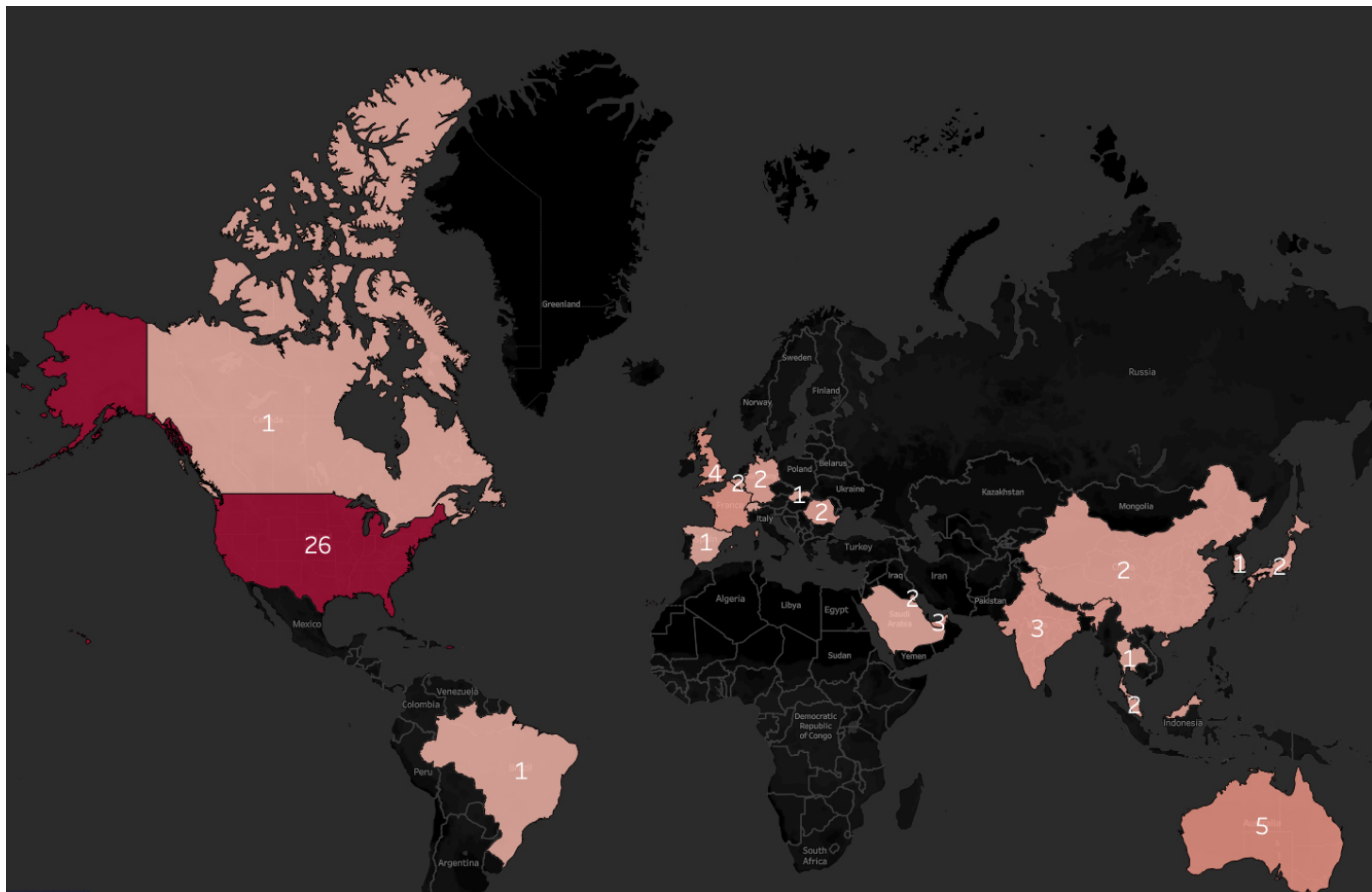
However, one noticeable blip exists far to the right, a threat actor selling unique access to an extremely high-value IT environment (backend access to a major auction house), in many ways this can be seen as whale hunting.

While the vast majority of access is low to medium value, occasionally extremely unique or high-value access is auctioned that can cause extreme pricing variation compared to our average. This was also on full display last year when threat actors attempted to sell 84 GB of European defense contractor and missile system data on Exploit for \$100,000 USD worth of bitcoin.

Higher priced listings often had access to unique environments or particularly sensitive files. However the vast majority of access was found in the form of RDP or VPN access to small companies and were priced fairly low.



# Geography Matters...Quite A Lot



Map showing number of IAB posts selling access to corporations globally, note that this map excludes instances where IABs listed the continent rather than country

A significant plurality of IAB posts were focused on U.S. companies, with the second most targeted country Australia at only slightly more than 1/7th of the volume of attacks against U.S. companies. This result was expected for several reasons:

- The U.S. has some of the most valuable companies in the world, in addition to the world's highest GDP making it a lucrative target for threat actors.
- Infostealer malware is likely a prime vector that initial access brokers use to establish access, in many cases infostealer variants are set to automatically disable when executed on hosts in a country belonging to the coalition of independent states (CIS), somewhat limiting potential countries for targeting.
- Exploit being a Russian forum, may deter threat actors from posting targets that are neutral or allied to Russia while incentivizing them to target countries hostile to Russia.

## Geography

USA	36.11%
Australia	6.94%
UK	5.56%
France	5.56%
UAE	4.17%
India	4.17%
Romania	2.78%
Malaysia	2.78%
Kuwait	2.78%
Japan	2.78%
Germany	2.78%
China	2.78%
Belgium	2.78%
Thailand	1.39%

Percentage of IAB posts selling access to corporations based in the respective countries



Next we wanted to explore how the “blitz” or buy it now price for listings changes by country. Our hypothesis was that blitz prices for access to U.S. companies would be substantially higher than non-U.S. companies due to economic differences, company valuations, and potential payments for ransomware and other cybercrime.

The presence of outliers can significantly skew the average, so we removed them using the interquartile range (IQR) method. The IQR is the range between the first quartile (25th percentile) and the third quartile (75th percentile) of the data. We considered any data point that falls below the first quartile minus 1.5 times the IQR or above the third quartile plus 1.5 times the IQR is considered an outlier.

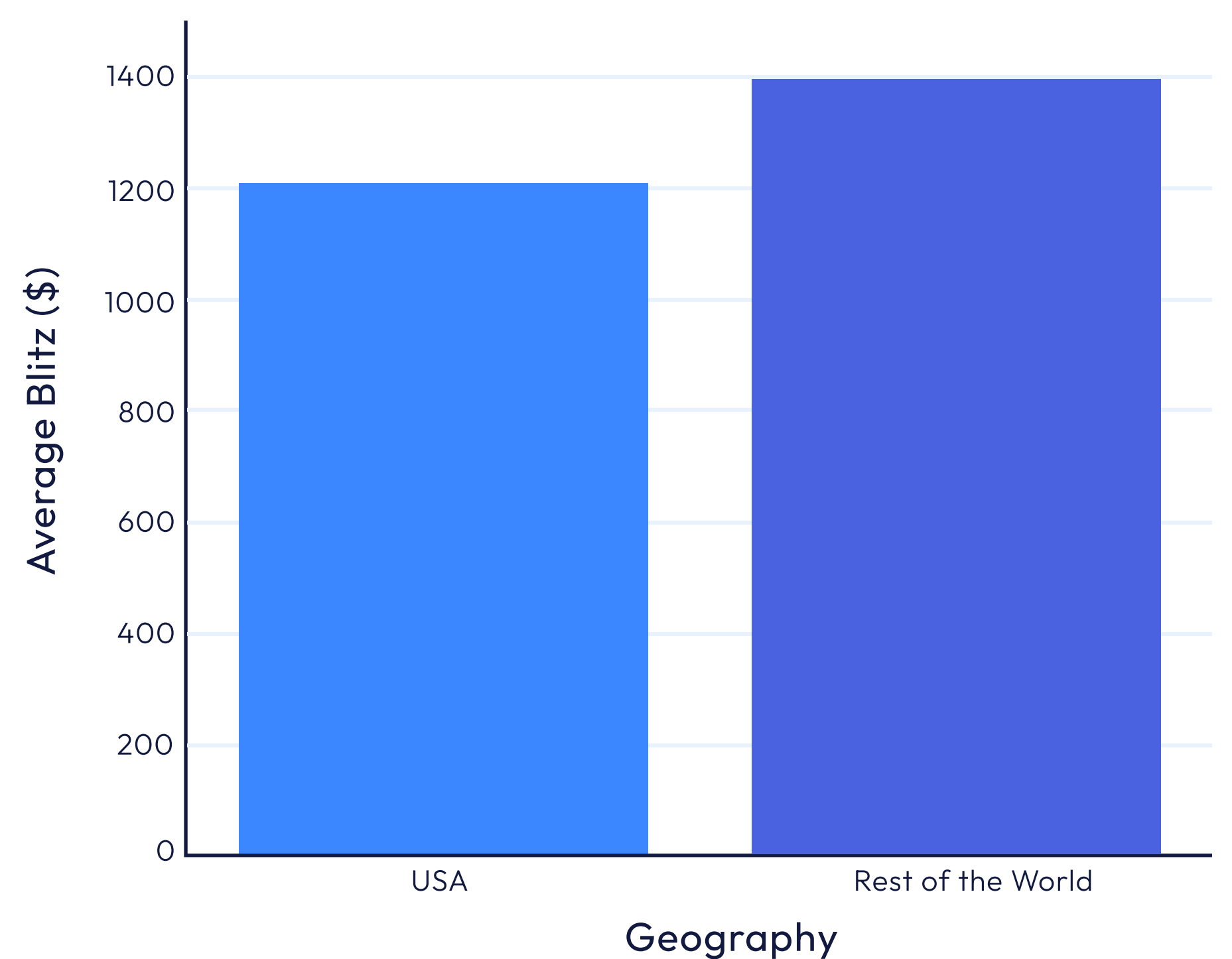
Our results showed that the average price, disregarding outliers, changes very little between organizations in the U.S. and the rest of the world. We were curious to test this hypothesis against data with outliers, to do this we incorporated outliers while removing a single extreme outlier.

This changed our results substantially with the average blitz price for U.S. companies significantly increasing to \$3,186, while the rest of the world increased to \$3,011.11. These changes represent the fact that there were several high blitz prices for both U.S. and international companies.

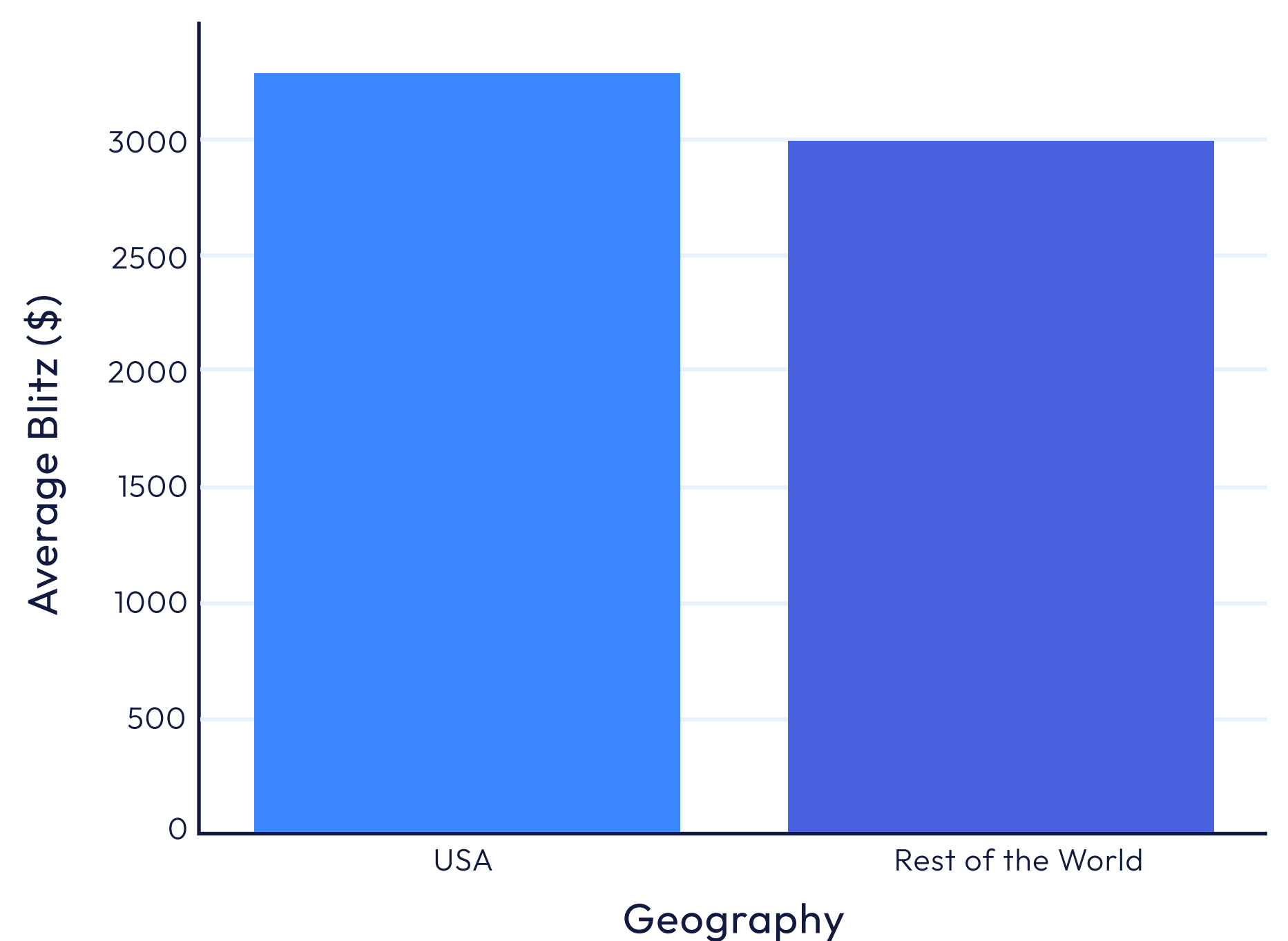
## Key Takeaways

- U.S. corporations are heavily targeted by initial access brokers, with 36% of victims advertised as being located in the United States.
- Australia and the UK were the second and third most targeted countries, representing 12.5% of our data set.
- After removing outliers, access to U.S. Corporations did not sell for significantly more or less than the global average, invalidating the hypothesis that U.S. companies would fetch a higher price than their global counterparts.
- The average blitz price for our data set after excluding outliers was \$1,328, while with outliers included it was more than \$3,000, indicating that occasionally access to a particularly valuable company is sold for multiple standard deviations about the average price, skewing results.

Average Blitz by Geography



Average Blitz by Geography (Highest Value Removed)





# How Many Threat Actors were Active During the Period?

Next we reviewed how many threat actors were actively selling access to corporate networks on Exploit during this period. We counted 31 unique usernames selling access to corporate IT environments; however the top seven actors were responsible for the majority (55.6%) of listings.

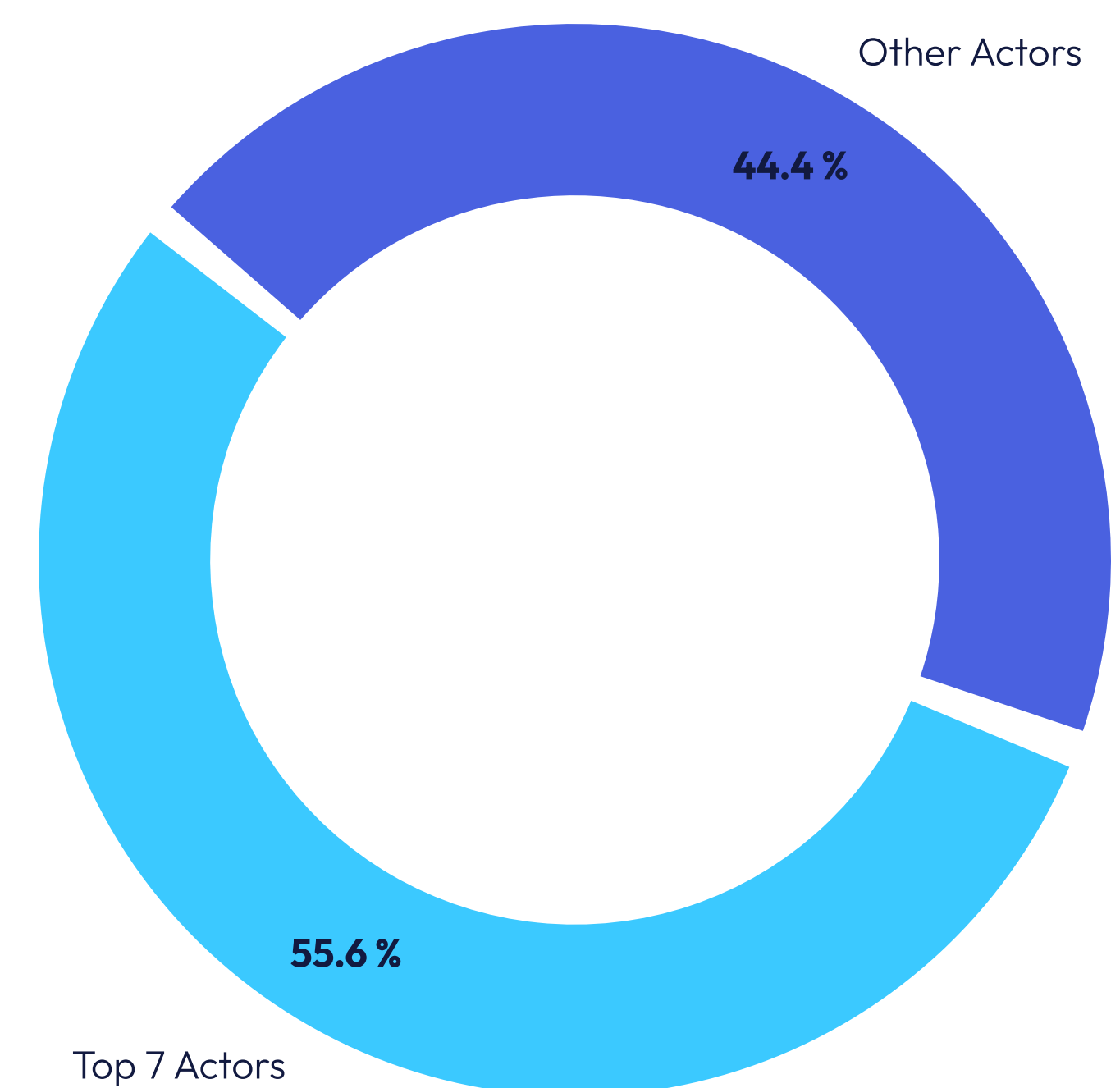
This could indicate that a select few threat actors have developed tactics, techniques, and procedures that enable them to gain access to a large number of IT environments compared to the average threat actor.

For this analysis we again used the IQR method to remove outliers and began by comparing threat actors based on their average blitz price. We also excluded actors that had a low sample size of events. We uncovered a substantial range in average blitz prices by actor, suggesting differences in targeting, level of access gained, and pricing strategy.

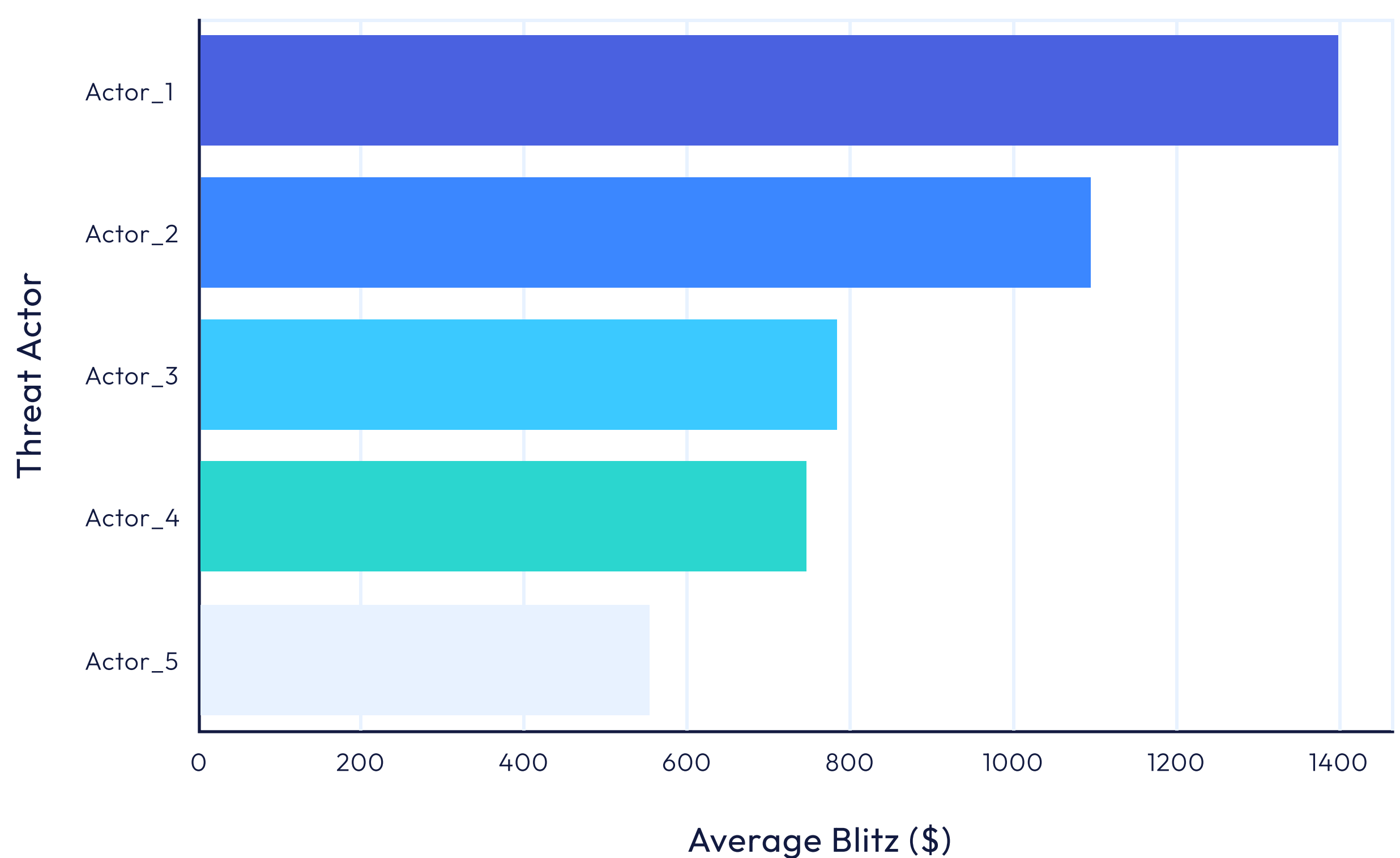
The average blitz price with outliers removed varied substantially between threat actors, with a range of \$558 to \$1,400. Given that the variances in company blitz price make it exceedingly unlikely that this range is driven by country targeting, we suggest the following explanatory factors.

- Some access brokers may focus on specific industries or verticals that yield a lower or higher average blitz price. This area represents an excellent opportunity for future research.
- Some IABs may lack the reputation to sell high-blitz price access, resulting in smaller sales to build reputation. Correlating the number of auctions an actor has held with the blitz price achieved is an interesting area for future study.
- The type of access being sold also significantly influenced price which will be explored later in this paper, some IABs may focus on particular types of access to environments, resulting in lower or higher selling prices.

Proportion of Listings by Top 7 Actors vs Others



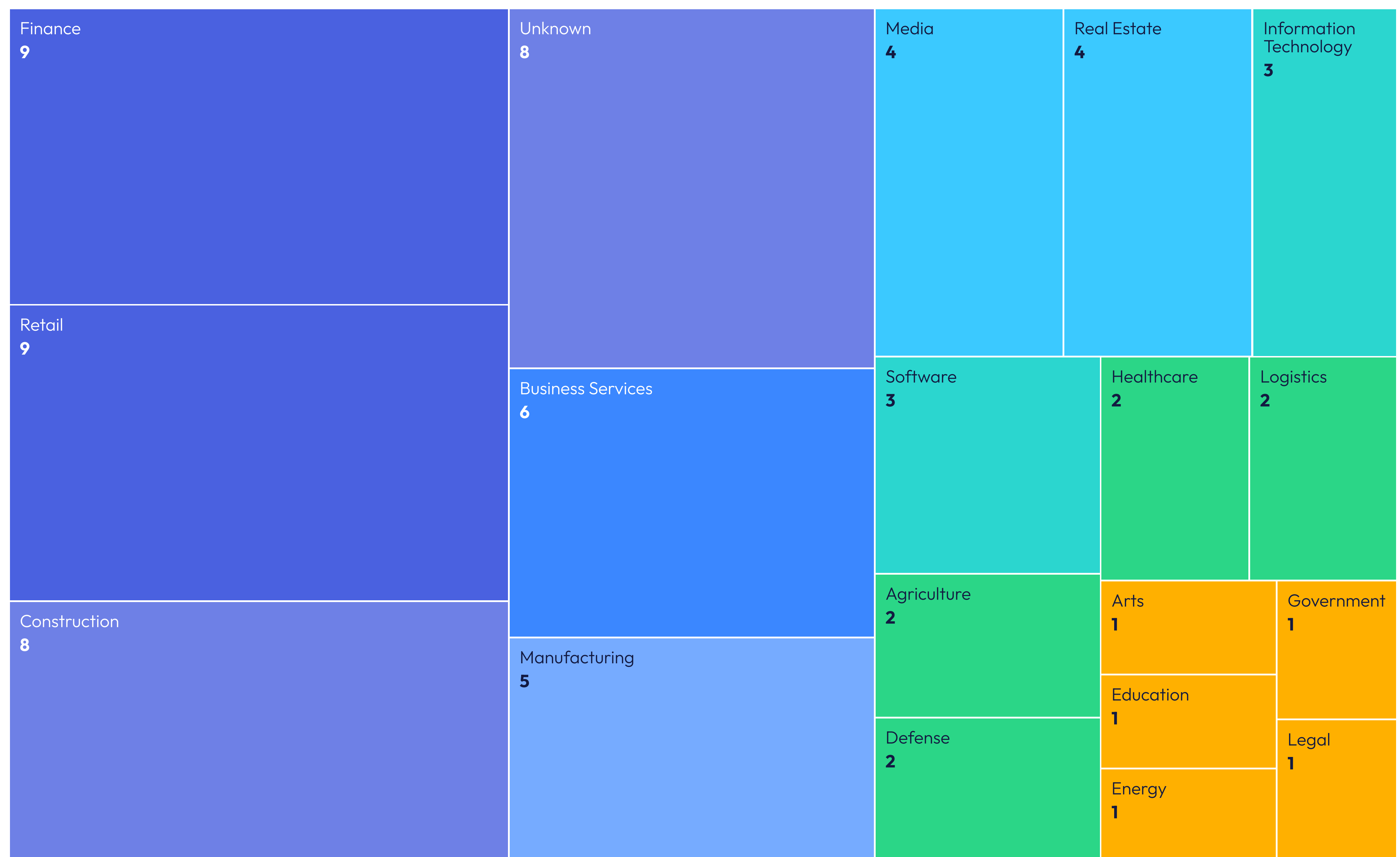
Average Blitz by Threat Actor (Anonymized)





# Initial Access Brokers & Industry

## Average Blitz Price by Industry

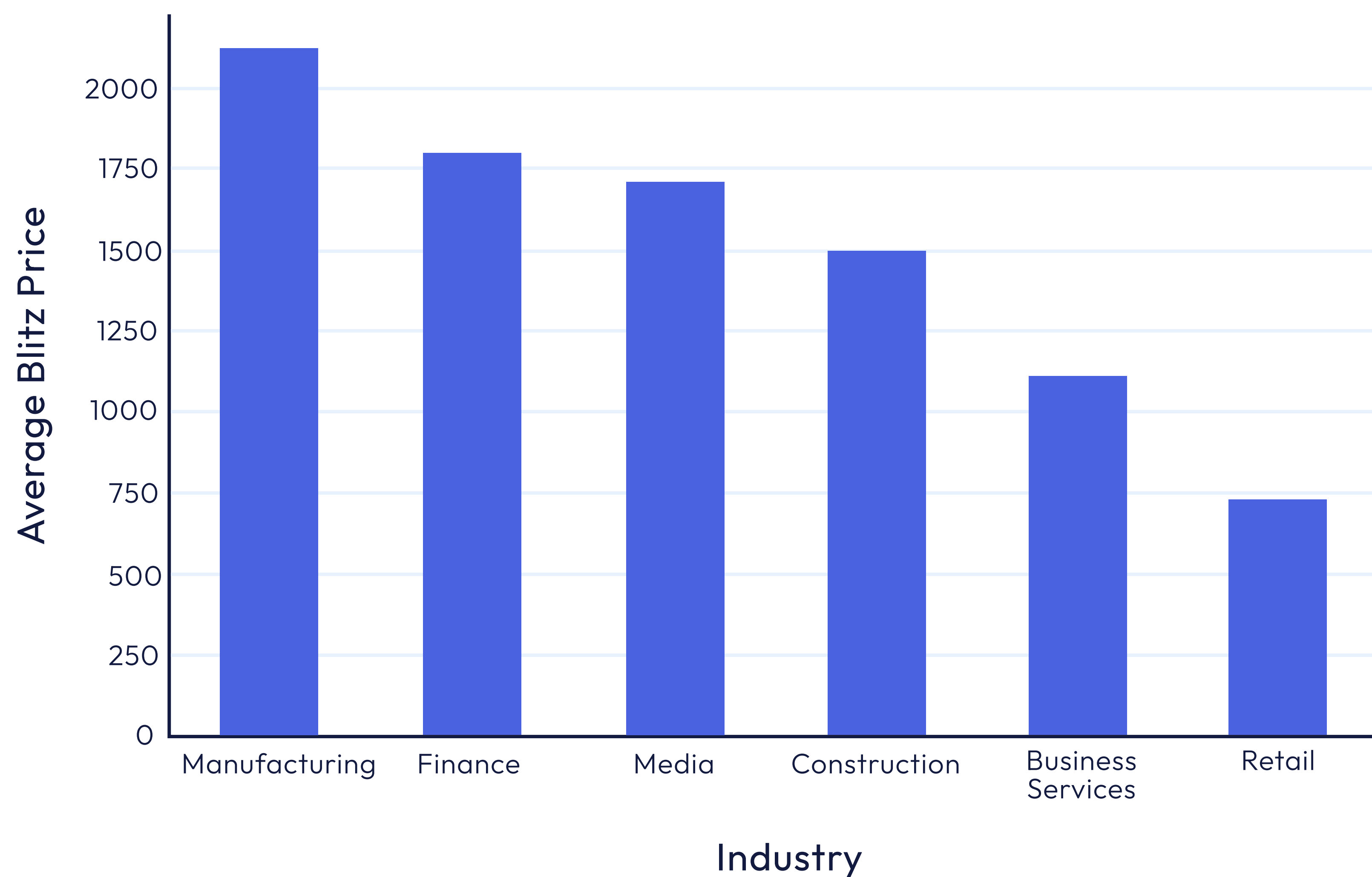


The average blitz price based on industry is another interesting data point that can help shed light on how IABs operate. Industry targeting plays a critical role in determining the value of initial access offerings. To do this, we classified organizations into 18 industries as depicted. Interestingly, unlike geographic location, the industry of the victim played a very substantial role in how the post was priced.

First we reviewed the average blitz price by industry (excluding outliers) where we found significant variation. We excluded posts with industry unknown and industries with less than four examples. Access to manufacturing sold for the highest price, coming in slightly above \$2,000 while access to retail organizations was sold at the lowest price, slightly under \$750.

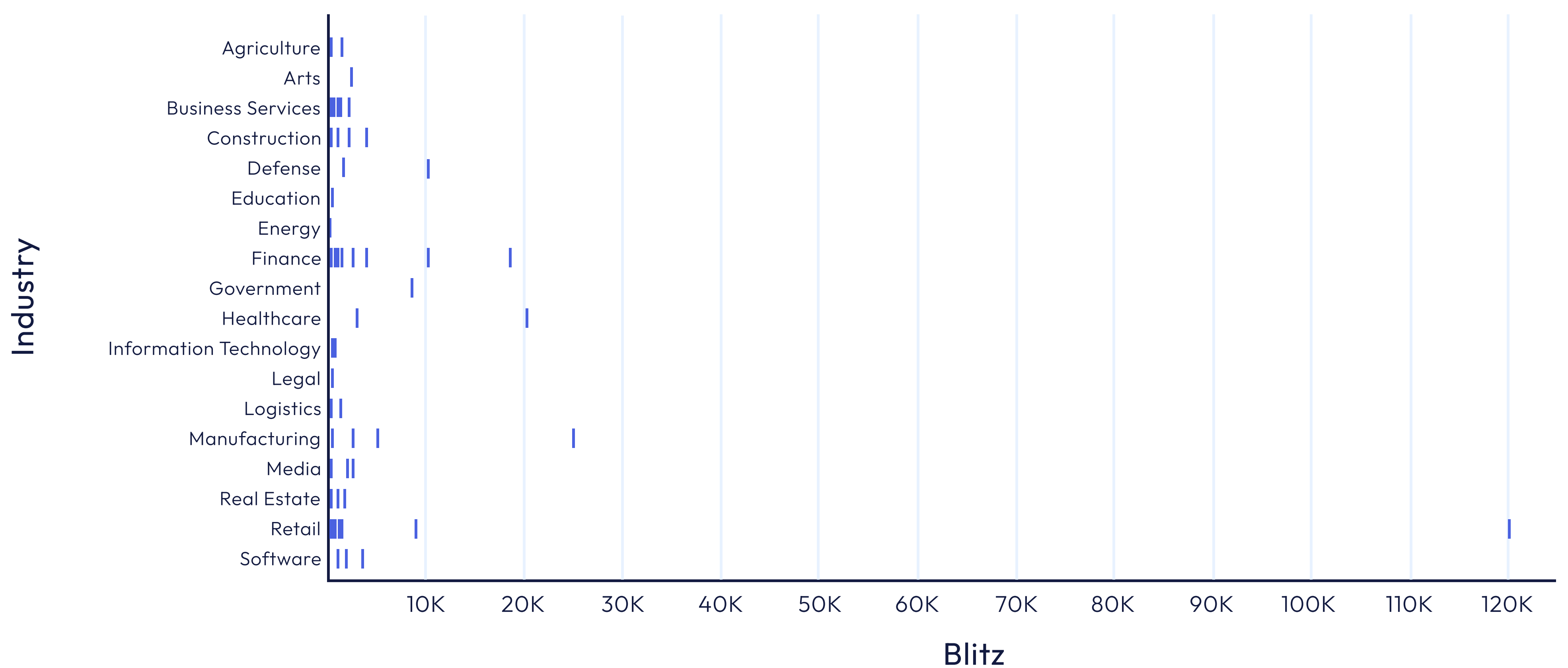


## Average Blitz Price per Industry (Excluding Outliers, Industries with Less Than 4 Records, and Unknown)



To further explore the relationship between industry and access price, we use a Gantt chart to visualize the distribution of IAB pricing by industry. The relative clustering for certain industries such as Media, Real Estate, Retail, and Business Services was striking compared to that of Manufacturing, Finance, and Defense, although this could be as a result of limited sample size and warrants further study.

## Distribution of IAB Pricing by Industry



Blitz price of all IAB posts (excluding unknown industry)



## Key Takeaways

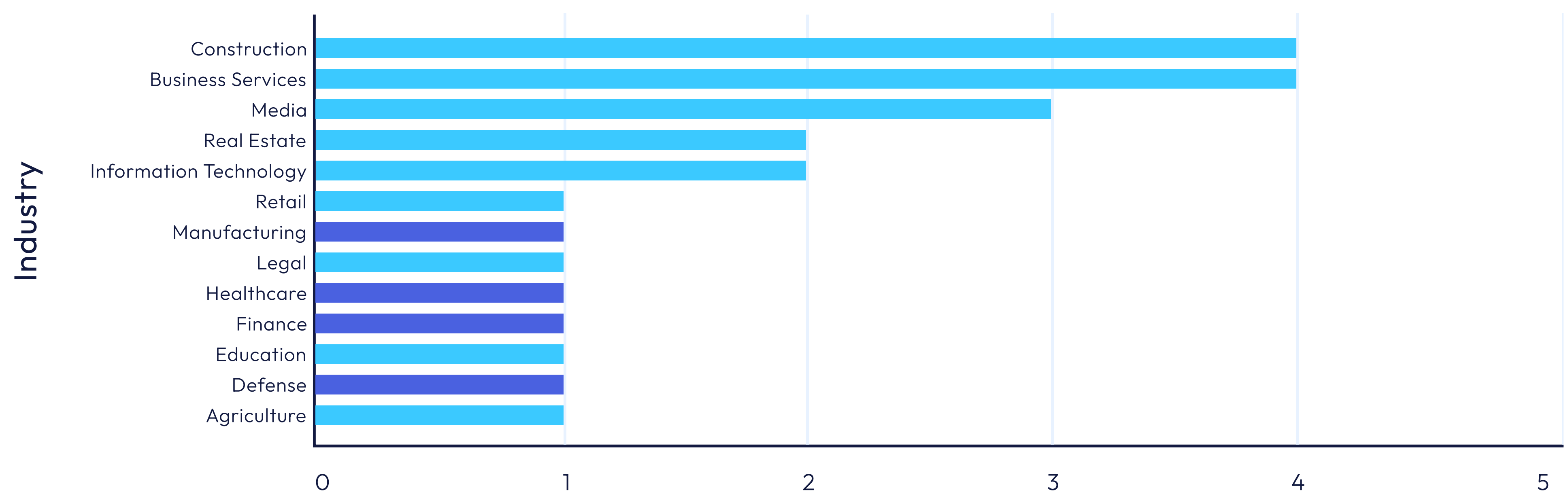
- Industry has a profound impact on pricing in our sample data, with certain industries selling for far higher average prices than others.
- Manufacturing, Finance, and Media access sold for the most, while Construction, Business Services, and Retail sold for the least.
- Price clustering around low \$1,000 and \$10,000 suggests that there are significant factors that can substantially increase the price for access to an organization.



# U.S. Critical Infrastructure, IABs, and Types of Access

We also wanted to look at the prevalence of IABs selling access to U.S. Critical Infrastructure. Initial access being sold to U.S. Defense Contractors, Financial Institutions, Healthcare Entities, and Food Suppliers can pose a significant risk to U.S. National Security. Our analysis detected five instances of access to U.S. Critical Infrastructure as defined by CISA sold on Exploit during the dates studied.

## IAB Posts by Industry (U.S. Companies)



Initial Access Broker Posts - U.S. Companies Excl Unknown Industry, Critical Infrastructure Highlighted

Interestingly for U.S. specific data, Construction and Business Services were the most affected industries.

The last data point we analyzed was the type of access being sold by threat actors. Many posts excluded this information, or used different naming conventions to explain the type and level of access making normalization across our data set difficult in some cases. In some cases actors would list the vector (such as compromised RDP) but not the level of access, in other cases they would combine level of access and vector, or simply list the level of access obtained.

By far the most common vector was RDP access, with 32 of 72 posts claiming that the type of access available was through RDP. The next most common vector was VPN access occurring 11 times. Combined these types of access represented 60% of listings within our data set.

The most common types of access obtained were administrator access to cloud environments (14 instances), local administrator privileges (five instances), and “user in domain” (two instances). In many cases non-standard access was obtained, such as to company specific SaaS applications, specific categories of data, and other IT applications. In a few examples we noted that threat actors specifically singled out that they were selling access to backup and recovery systems in addition to corporate IT access, indicating that the access was likely intended to be used for ransomware operations.



## Key Takeaways

- Access to U.S. Critical Infrastructure is routinely sold on Exploit but not overrepresented compared to other industries.
- IABs sell access which affects organizations across a range of industries including Finance, Manufacturing, Defense, and Healthcare.
- Access to RDP and VPN accounted for the vector in 60% of all initial access broker posts.
- The most common level of access was for administrative access to cloud environments, followed by local administrator privileges and “user in domain.” Oftentimes, the level of access was omitted or contained a unique value.



# IABs and Russian Hacking Forums - An Urgent Call to Action

Initial access brokers represent a real and present threat to companies globally. Threat actors operating on Exploit forum are auctioning off access to a new company almost daily, and Exploit only represents one of multiple forums with initial access broker activity. We recognize that many recommendations are uniform across security reporting such as establishing MFA controls, training users, and performing other basic security practices. In addition to those, we strongly recommend that organizations:

- **Monitor IAB Forums:** As noted, IAB posts are almost entirely anonymized to avoid tipping off victims, however the combination of geography, revenue, industry, and type of access may be enough information to provide some organizations advanced notice that they have potentially been compromised. We recommend monitoring Exploit, XSS, and other IAB forums to receive advanced notice that access to your environment may be for sale.
- **Put Monitoring in Place for Stealer Logs:** We expect that stealer logs represent a significant source of vectors for IABs. It is highly likely that threat actors sort through enormous numbers of logs to find those with RDP, VPN, and other forms of corporate access which can be established, expanded, and resold. We recommend monitoring across public & private Telegram channels, Russian Market, and Genesis Market.
- **Automate Public GitHub Secrets Detection:** We have not firmly established a link between public GitHub secrets leakage and access broker posts, however developers copy pasting code into public repositories containing credentials represents a potential vector of access for IABs.



# About Flare

Flare is the proactive external cyber threat exposure management solution for organizations. Our AI-driven technology constantly scans the online world, including the clear & dark web, to discover unknown events, automatically prioritize risks, and deliver actionable intelligence you can use instantly to improve security.

**Want to learn about how Flare can support monitoring for IAB activities?**

[Free Trial](#)

[Book a Demo](#)

[flare.io](https://flare.io)

[hello@flare.io](mailto:hello@flare.io)

