# Access Brokers: Their Targets and Their Worth

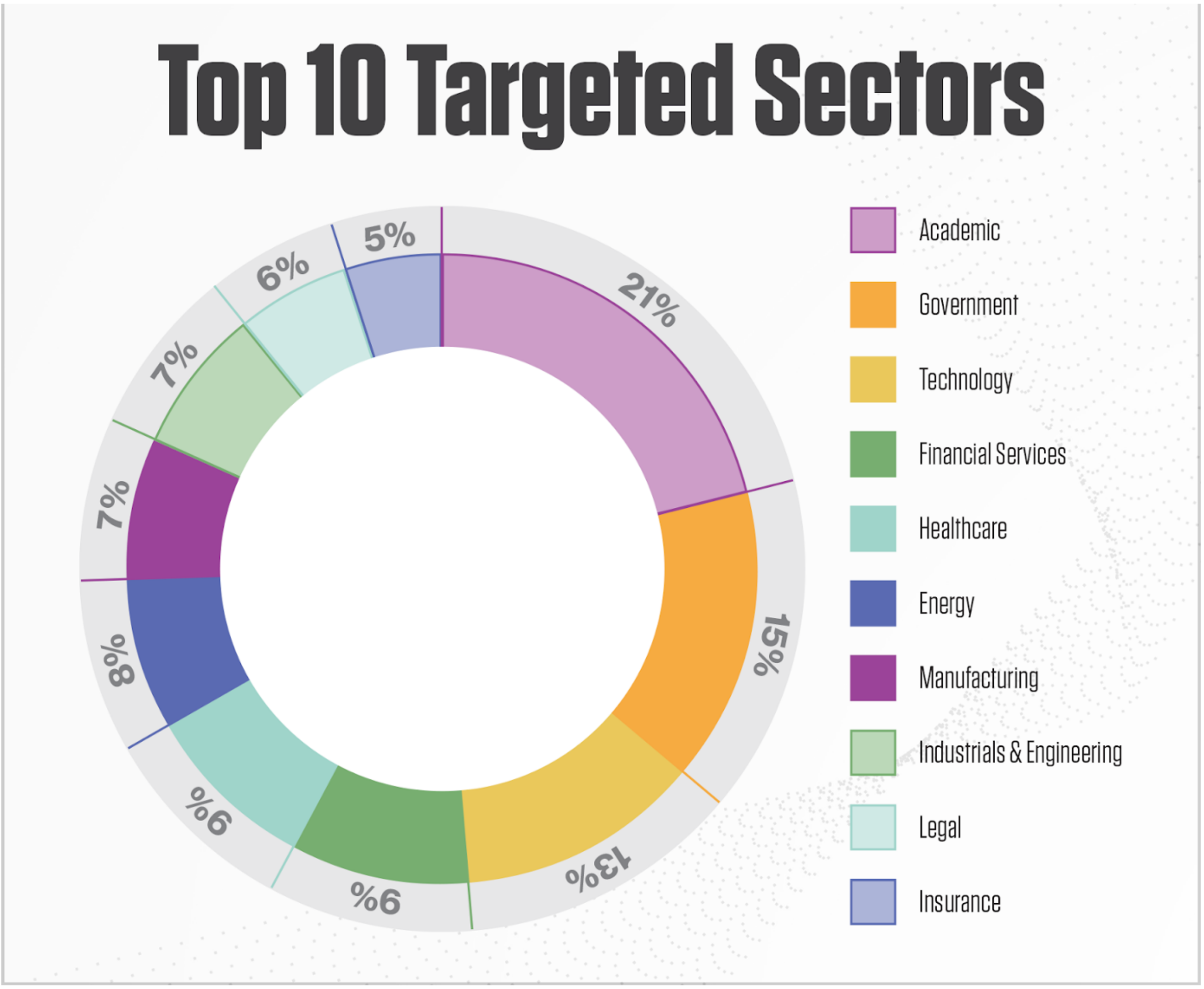
crowdstrike.com/blog/access-brokers-targets-and-worth/

CrowdStrike Intelligence Team

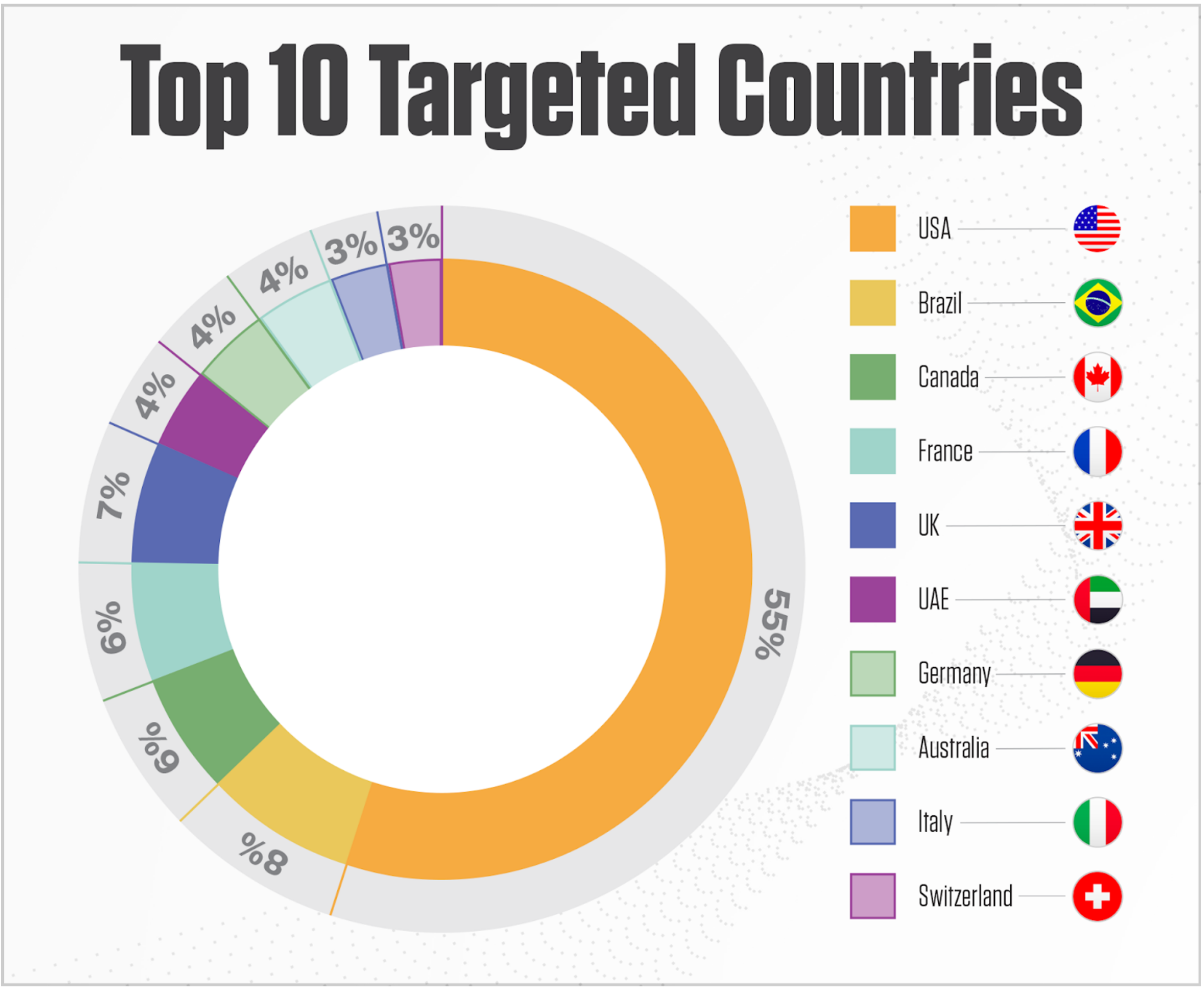
February 23, 2022

Access brokers have become a key component of the eCrime threat landscape, selling access to threat actors and facilitating myriad criminal activities. Many have established relationships with big game hunting (BGH) ransomware operators and affiliates of prolific ransomware-as-a-Service (RaaS) programs. The CrowdStrike Intelligence team analyzed the multitude of access brokers' advertisements posted since 2019 and identified trends in targeting preferences, as well as insights into the perceived value of different victims.

## Top Targets



Top 10 Targeted Sectors



Access brokers have advertised organizations from more than 30 different sectors, demonstrating an eclectic range of targets. Among these, the academic, government and technology sectors were the most frequently advertised, accounting for a combined 49% of the total advertisements.

The academic sector has historically been a popular focus of ransomware operations, with intrusions timed to coincide with the start of a new school term to cause the greatest disruption and in turn encourage a quick ransom payment. Almost 40% of the academic sector advertisements were for access to U.S.-based institutions, with a spike in activity noted in August 2021 that coincides with the start of the new semester.

Geographically, advertisements for access to U.S.-based entities far surpass those for all other countries, claiming 55% of the total. Organizations based in Brazil and the UK secure second and third spots with 8% and 7%, respectively.

This geographic targeting trend corresponds with other eCrime activity, including data theft campaigns that frequently result in stolen credentials being traded online in criminal underground marketplaces. Access brokers are known to purchase such credentials and abuse them to acquire access.

## Controversial Targets

The healthcare sector has been a divisive target among eCrime actors during the past two years because of the COVID-19 pandemic. Some adversaries actively avoided operations against frontline services in particular. Access brokers showed varying interest in targeting the sector — it sits in joint fourth place alongside financial services for the total number of identified advertisements, but the timing of the advertisements fluctuated.

Only one advertisement was posted for a healthcare entity in Q1 2020 — coinciding with the emergence of the pandemic — yet several were posted in Q3 2020 and Q1 2021. The increase corresponded with news of successful vaccination programs, potentially prompting increased interest among eCrime adversaries. Law enforcement scrutiny of cybercrime targeting critical infrastructure, which includes healthcare, also likely impacted supply and demand for access to this sector.

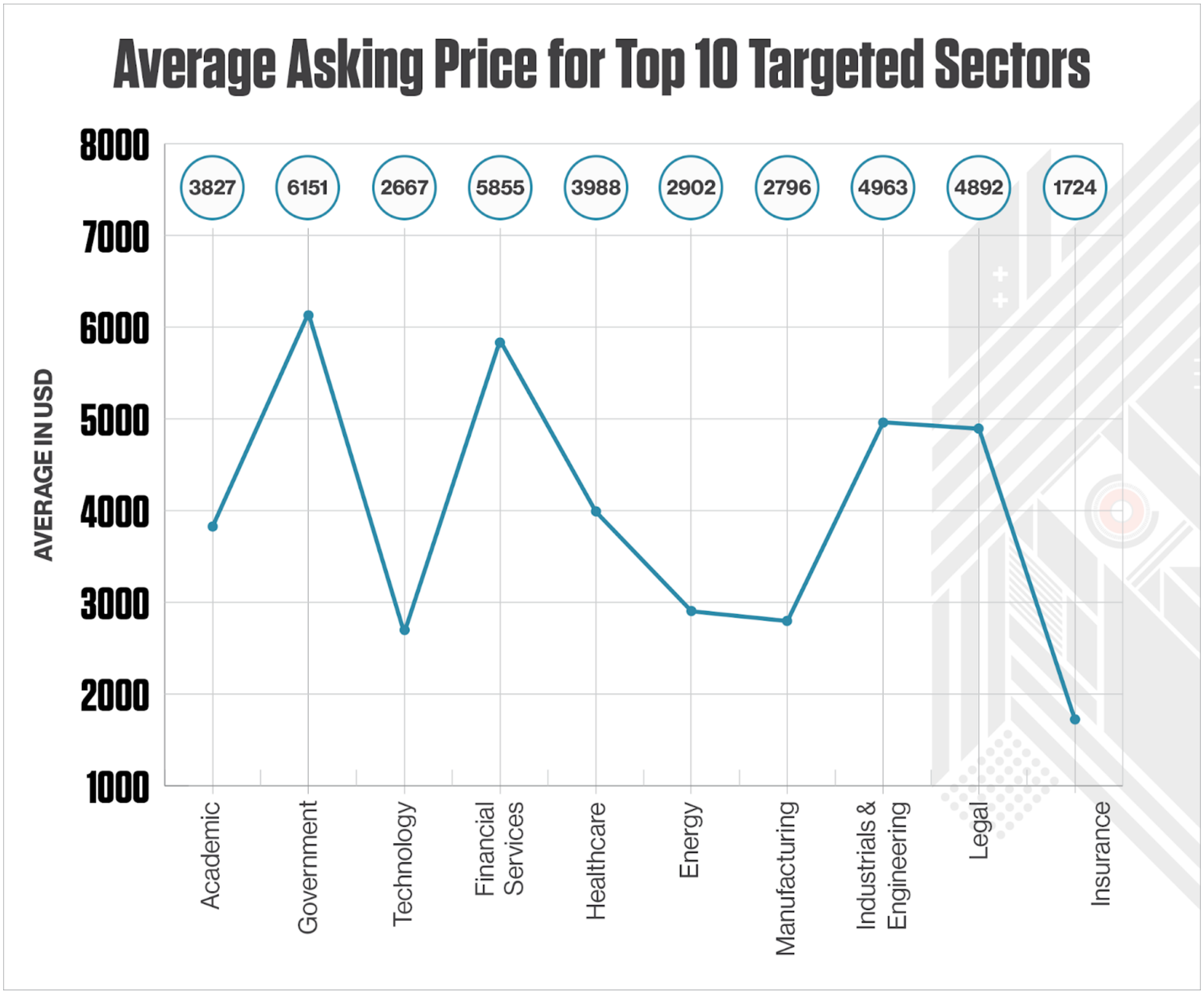
The energy sector was another controversial target in 2021. The fallout from the *Darkside* ransomware incident against Colonial Pipeline in May 2021 had a knock-on effect on access brokers, as criminal forum moderators imposed restrictions on ransomware-related discussions. Since ransomware operators account for a high proportion of access brokers' customer base, the ban likely impacted sales for some brokers. Many switched to private communication channels, selling only to trusted buyers and hindering efforts to track who was selling to whom.

Despite the Colonial Pipeline incident prompting these changes, demand for access to the energy sector never truly waned, though the asking price for access briefly dipped.

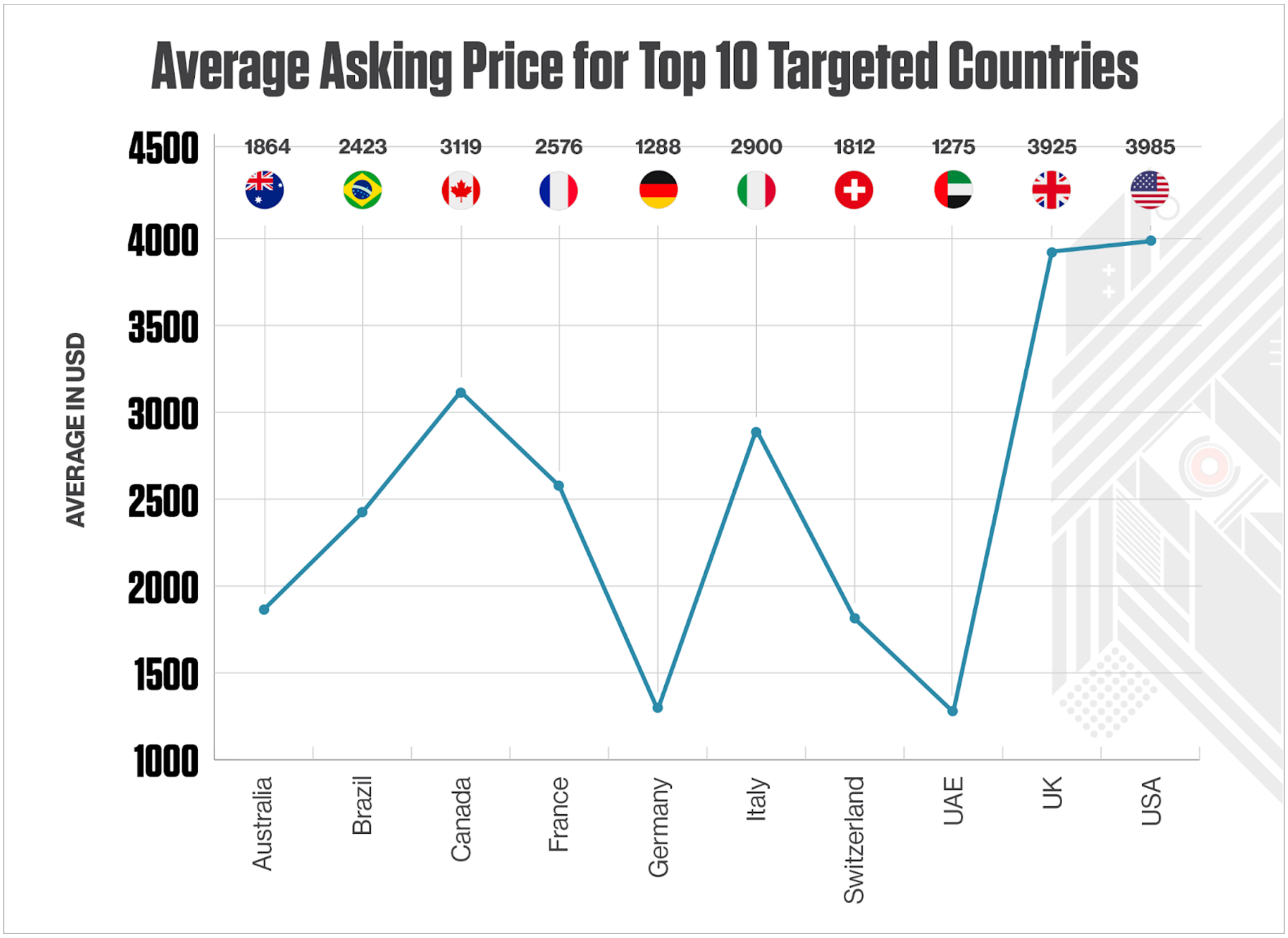
## What Is Access Worth?

Several factors determine the worth of access, and asking prices vary significantly among sectors, countries and access brokers. Access with elevated privileges typically attracts a higher asking price, as does access to large corporations with higher annual revenues or advertisements by more-established access brokers. Some brokers auction the access, offering a "buy-it-now" price or attempting to encourage a bidding war.

The sectors attracting the highest average asking price for access were government, financial services, and industrial and engineering organizations. The most advertised sector does not necessarily attract the highest asking price; for example, access to the academic sector was, on average, priced at $3,827 USD. In comparison, the government sector — which was the second most advertised — attracted an average asking price of $6,151 USD.



Organizations based in the U.S., the UK, and Canada on average attracted higher asking prices than other countries, reflecting the demand in targeting these locations. It is worth noting that the advertised price is not necessarily what's paid, and the majority of access brokers appear open to negotiation.



Fluctuations in asking prices are also common and often reactive to the market. CrowdStrike reported an increase in asking price among access brokers in April 2021, with some corporate entities attracting five-figure sums, indicating that threat actors likely receive a significant return on their investment. When the same access is being advertised by two different access brokers, variations in the asking price are also observed.

## Conclusion

The advertisements provide an interesting snapshot of an increasingly lucrative component of the eCrime ecosystem, where reputation and timing both play important roles. There is almost certainly an opportunistic element to access broker operations, such as the availability of exploitable vulnerabilities or the validity of stolen credentials that facilitate intrusions.

The fallout from the Colonial Pipeline incident and its impact on access brokers' sales appears to have been short lived, as in Q4 2021 and Q1 2022 CrowdStrike Intelligence has witnessed a resurgence in advertisements and the emergence of new brokers. Purchasing access saves time and resources for many eCrime adversaries, and the demand for these is almost certain to remain high throughout 2022.

Falcon X Recon, CrowdStrike’s digital risk protection solution, goes beyond the dark web to include forums with restricted access on the deep web, breach data and messaging apps — all resources commonly used by access brokers to trade or advertise. Falcon X Recon provides customers with an increased level of situational awareness and helps uncover potential malicious activity before eCrime adversaries have the chance to exploit it.

The CrowdStrike eCrime Index (ECX) also remains a valuable tool used to identify significant events that affect the eCrime ecosystem, including fluctuations in the value of accesses. Monitor the ECX regularly in the CrowdStrike Adversary Universe to make sure you stay up to date on these trends.

## Additional Resources

- *Learn more about CrowdStrike Falcon X Recon by visiting the product webpage and downloading the data sheet.*
- *Find out how to stop adversaries targeting your industry — schedule a free 1:1 intel briefing with a CrowdStrike threat intelligence expert today.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ to see for yourself how true next-gen AV performs against today’s most sophisticated threats.*