flare

The Account and Session Takeover Economy

Defining exposure, costs, and impact of compromised end user accounts.

Executive Summary

Session hijacking has emerged as the preeminent way for cybercriminals to execute account takeover attacks (ATO) and they enable the bypassing of traditional security measures like multi-factor authentication (MFA). This research report explores the prevalence of session hijacking across industries, highlighting its increasing role in ATO incidents and the economic impact it poses for organizations.

Key findings from the report include:

- **Exposure rates vary by industry**, with **social media**, **cloud applications, and entertainment platforms** having the highest numbers of average monthly compromised sessions
- The average annual growth rate of exposed accounts is 28% which is largely tied to the proliferation of infostealer malware
- The **economic impact of ATO and session hijacking is significant,** factoring in:
  - **Labor costs** for security investigations (~$26.2M annually for a large streaming platform)
  - **Fraud losses** from account takeovers (~$7.5M annually)
  - **Customer churn risk**, which can lead to **tens of millions in lost revenue** each year.

This report underscores the urgent need for proactive ATO prevention strategies, emphasizing the role of **automated identity intelligence, session re-authentication policies, and early exposure detection** in mitigating the risks associated with session hijacking.

Session Hijacking – "The Path of Least Resistance" to Account Takeovers (ATO)

An account takeover (ATO) attack is exactly what it sounds like—when a cybercriminal or threat actor gains unauthorized access to an account for a web application. Whether the account is personal or a corporate asset, attackers have numerous ways to exploit or monetize stolen credentials. This report primarily focuses on personal accounts, examining how ATO impacts some of the world's most widely used web applications, most of which are business-to-consumer (B2C) rather than business-to-business (B2B) products.

Attackers have historically used several methods to take over accounts, including phishing, social engineering, leveraging credential leaks, brute-force attacks, or simply guessing weak passwords. Over the years, account security has improved significantly, with password complexity requirements, login attempt limits, and multi-factor authentication (MFA) becoming standard, even for consumer applications.

However, one technique remains largely unaffected by these security measures: session hijacking. This method exploits session cookies or tokens—technology designed to improve user convenience—against the user. Despite being a well-known technique, session hijacking has played a role in major breaches, including the 2023 Okta[1] incident. The fact that even reputable cybersecurity companies have fallen victim to this method underscores the difficulty of defending against it.

[1]ManageEngine. (2024, January 25). Understanding the Okta supply chain attack of 2023: A comprehensive analysis. ManageEngine IT Security Blog. https://blogs.manageengine.com/it-security/2024/01/25/understanding-the-okta-supply-chain-attack-of-2023-a-comprehensive-analysis.html

In 2024, Google researchers reported that session cookie-based attacks occur as frequently as password-based attacks[2]. The increasing prevalence of session hijacking can be simply explained through the classic "motive, means, and opportunity" framework for analyzing crime (see Figure 1). This technique sits at the intersection of:

- **Lucrative financial incentives** (covered later in this report).
- **Widespread availability of low-cost or free tools** that allow attackers to easily replicate browser sessions, often referred to as “anti-detect” browsers.
- **Infostealer malware** operations which Flare has reported on in depth over the years. “Stealer logs” containing compromised session tokens and credentials kick off the flywheel of opportunity by providing a steady supply of fresh stolen data that can be leveraged in attacks.

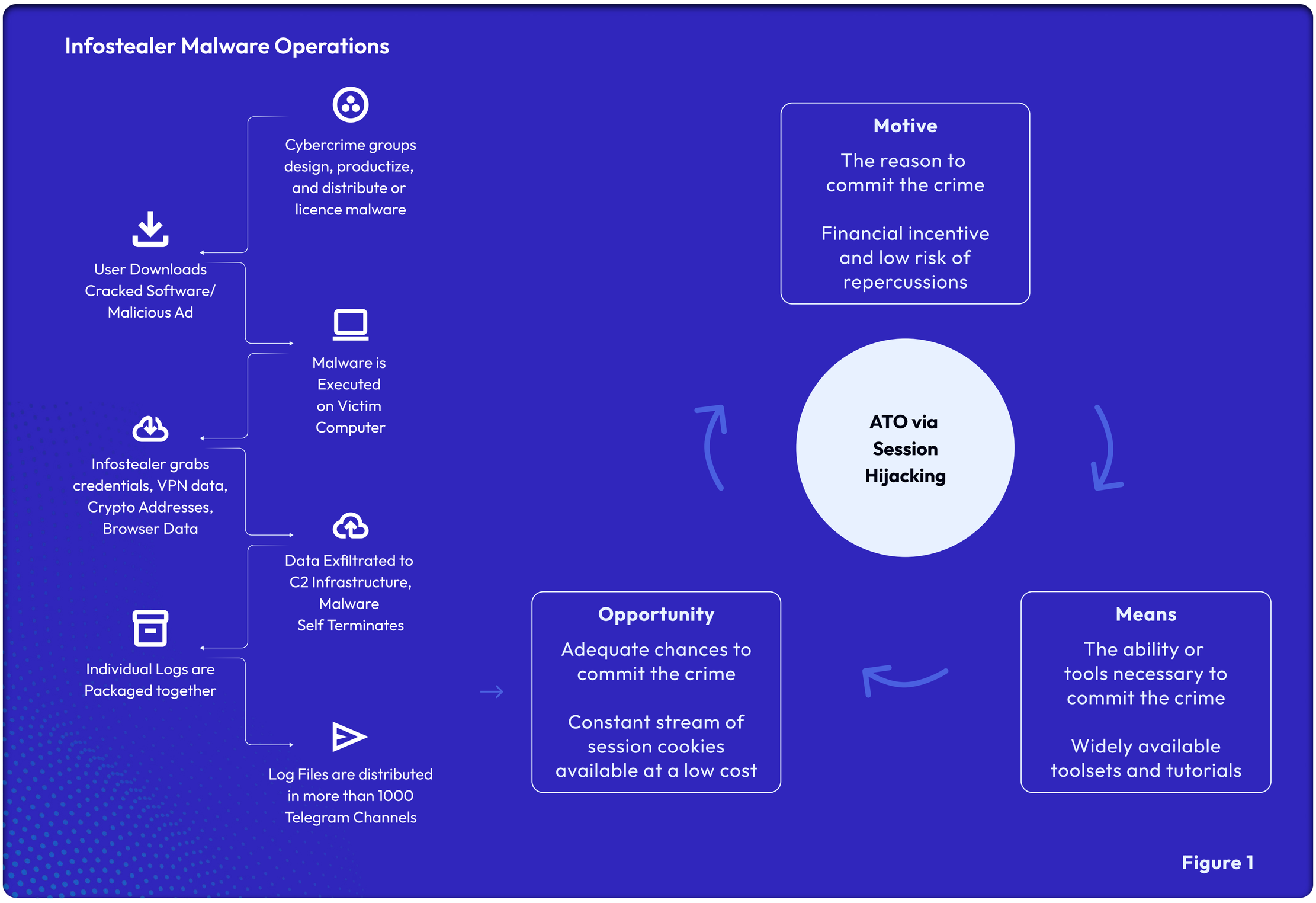


Figure 1

[2]W3C Web Application Security Working Group. (2024). Discussion on database-stored credentials security [Comment on Issue #13]. GitHub. https://github.com/w3c/webappsec-dbsc/issues/13#issuecomment-1977657864

Session Hijacking Exposure by Industry

Data Preface

The data you will find in this section is largely based on infected devices. In other words, devices where infostealer malware was successfully executed and browser data was extracted. The data is based on collection efforts spanning approximately four years. For simplicity, we recommend assuming one exposed device corresponds to one exposed account. While it's certainly true that a number of infected devices may contain multiple exposed accounts for the same application, and a number of exposed accounts may appear on multiple infected devices, these subsets are assumed to more or less balance each other out. This 1:1 estimation provides a reasonable, albeit imperfect, baseline into ATO and session hijacking exposure. The data focuses on over 100 of the world's most widely used web applications, broken down by industries and sub-industries, with company names anonymized.

ATO Exposure Rate

For these figures, we took a random sample of 20 of the 100 web applications across multiple industries. Estimated end users for each web app ranged from 5 million to 300 million.

1.4%

Median Web App ATO Exposure Rate

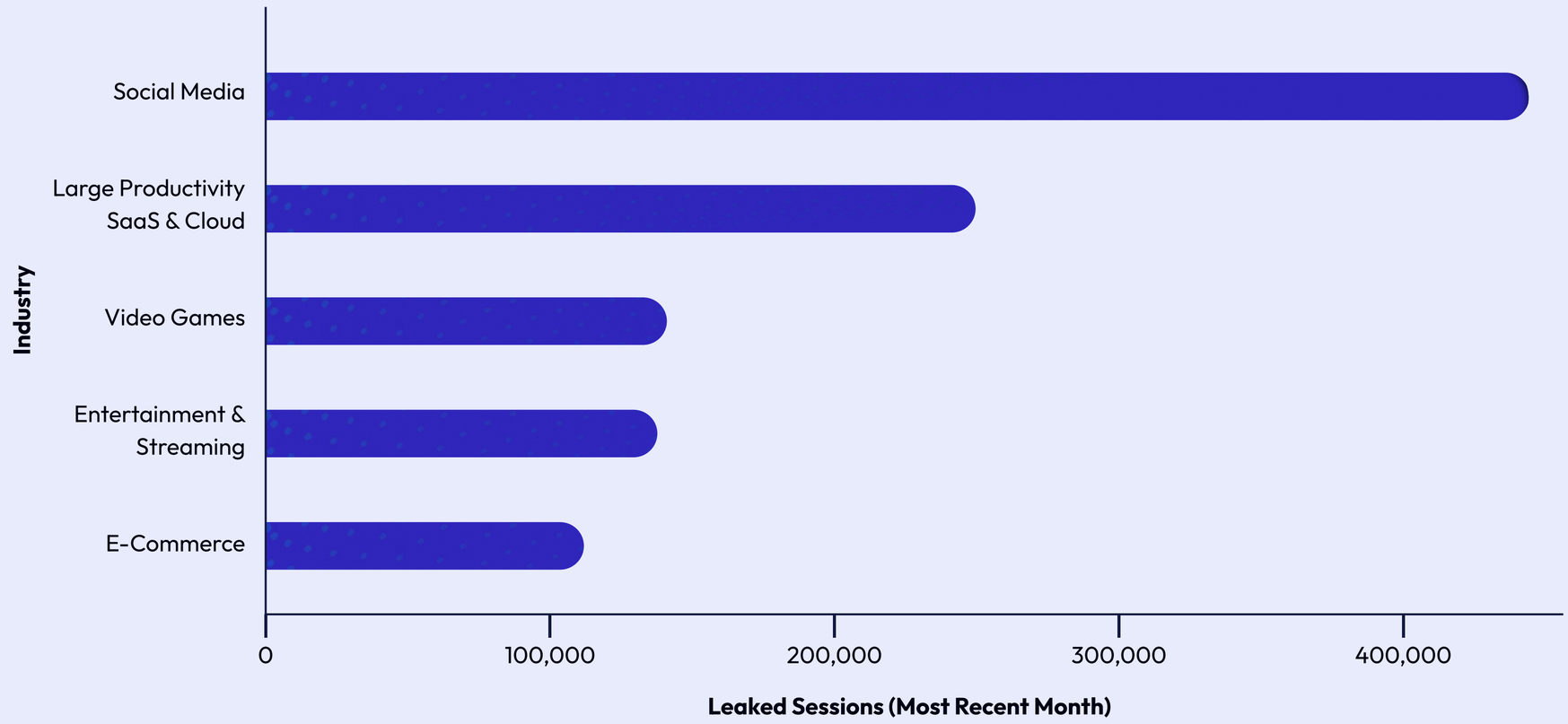
2.1M

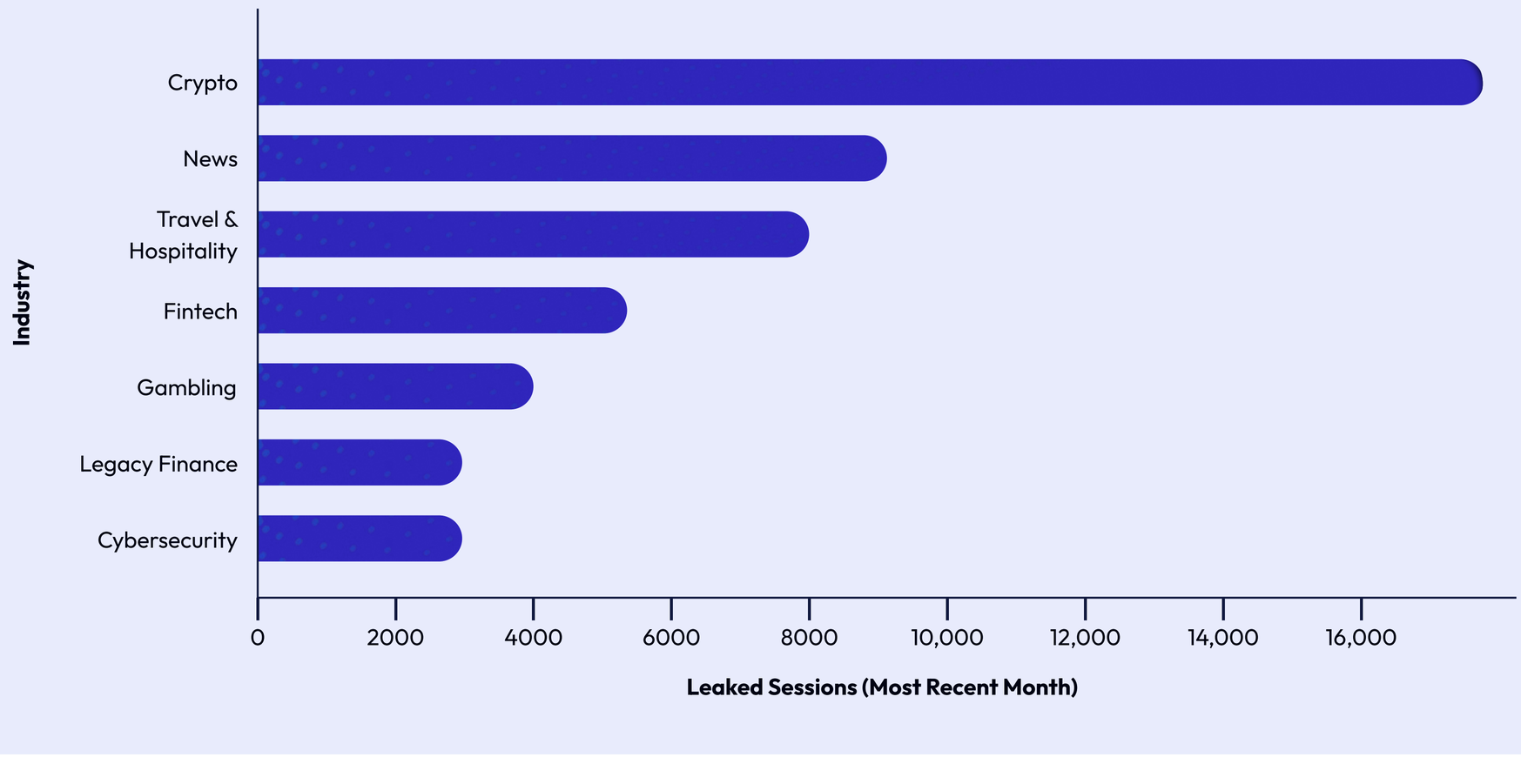
Median exposed user accounts

Average New Exposed Accounts (Monthly)

Industry	Average Monthly Exposed Sessions
Social Media	462,000
Large Productivity SaaS & Cloud	239,000
Video Games	142,000
Entertainment & Streaming	140,000
E-Commerce	109,000
Crypto	17,000
News	9,000
Travel & Hospitality	8,000
Fintech	5,000
Gambling	4,000
Banking	3,000
Cybersecurity	3,000

Average New Exposed Accounts (Monthly) - Scaled View





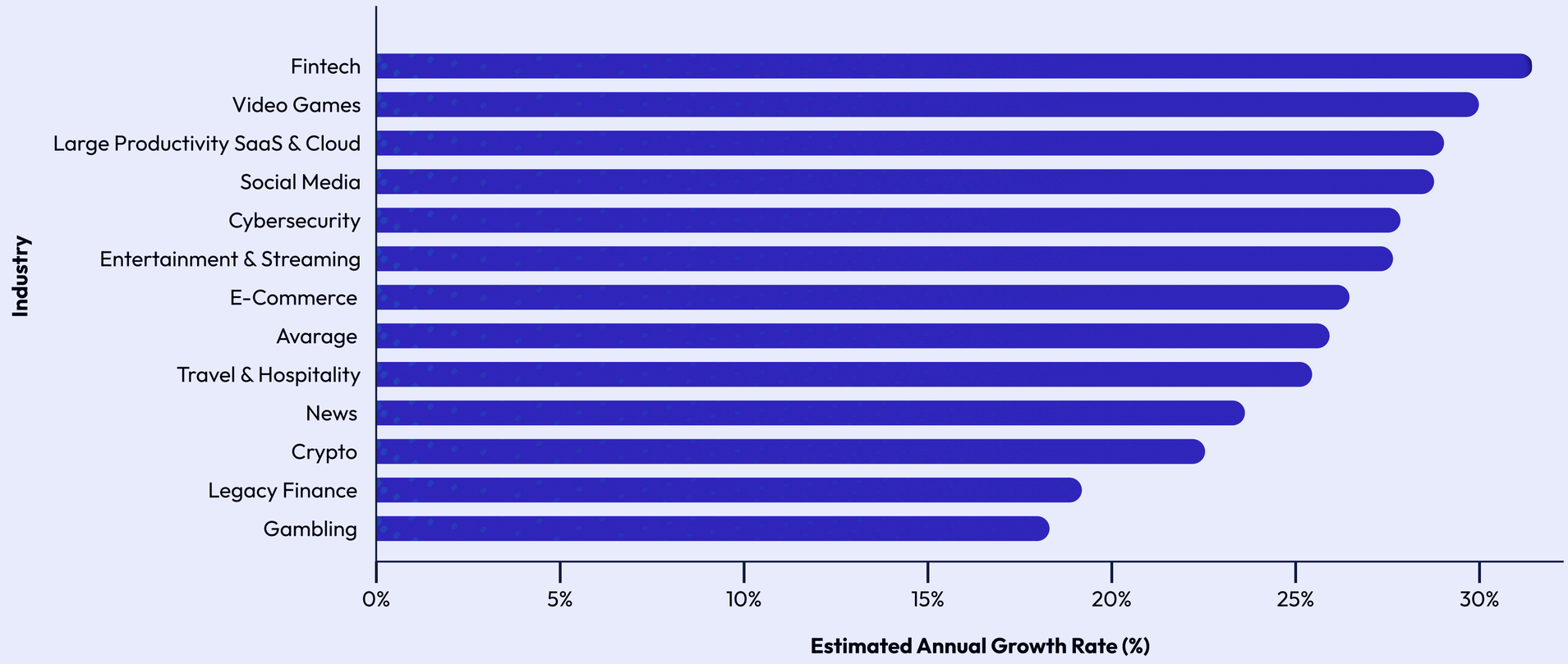
Observations

- There is a clear correlation between the number of users a web application has and its exposure within Flare's database. Large social media platforms, with hundreds of millions of users worldwide, tend to have higher exposure, whereas cryptocurrency exchanges and gambling websites typically have a smaller user base and correspondingly lower exposure.
- It is important to consider the inherent device bias in this dataset. In most cases, these accounts were leaked from a browser on a Windows laptop or desktop rather than a mobile device like a smartphone or tablet. As a result, applications primarily used on mobile devices are underrepresented in this dataset.
- Additionally, stricter policies around session cookies and authentication contribute to the relatively low exposure observed in cybersecurity, banking, and gambling applications.

Estimated Annual Growth Rate in Exposed Devices

The following data is based on Flare's collection efforts dating back to 2021. This growth rate is a reflection of the annualized year over year growth of exposed accounts over the past four years.

Estimated Annual Growth Rate in Exposed Accounts	
Fintech	32%
Video Games	30%
Large Productivity SaaS & Cloud	29%
Social Media	29%
Cybersecurity	28%
Entertainment & Streaming	27%
E-Commerce	26%
Travel & Hospitality	26%
News	24%
Crypto	22%
Legacy Finance	19%
Gambling	18%



Observations

- Fintech or financial technologies representing the highest growth rate could be a sign of both increased worldwide adoption of these services and increased attacker opportunity.
- Gambling coming in at the lowest growth rate is interesting, considering the explosion in growth and visibility that industry has seen in North America. The aforementioned authentication practices and device bias could account for this.

Quantifying the Economic Impact of Session Hijacking for Large Web Apps

Precisely quantifying the economic impact of session hijacking is challenging. To help organizations estimate their risk, we've developed an ROI calculator that breaks down web app exposure by industry. By multiplying the average monthly exposed accounts by the approximate cost of a single account takeover, organizations can derive a baseline estimate of risk exposure to active sessions. It's important to note that this calculator is by no means exhaustive, and other factors - namely labor, fraud, and customer churn - must be considered to gain a comprehensive understanding of session hijacking risks.

Labor

Labor is a simultaneously obvious and yet under-quantified cost. In 2023, Amazon disclosed that they invested over $1.2 billion and dedicated over 15,000 employees to fraud and abuse[3], implying over 25 million working hours per year. Only a select few companies in the world have these kinds of resources, however. A better way to think about labor costs is on a per investigation basis, which we've broken down in the box below.

Account Takeover Investigation Cost Assumptions

- **Hourly rate assumption:** $60-$75.
  - Assumes a $130K - $150K "fully loaded" salary and additional compensation package for a cybersecurity or fraud/risk professional.
- **Time spent per true-positive investigation:** 30 Minutes to 1 Hour.
  - Assumes time spent triaging alerts from detection tools, correlating data from threat intelligence sources and internal logs, and any relevant cross functional communication that occurs before an action is taken.

In practice, an investigation could be faster (30 minutes, $30–$40) if it's straightforward, or slower (2 hours, $130–$150) if it's complex. But **$70** is a good baseline average for labor on a single account takeover investigation.

By multiplying $70 dollars by the number of annual account takeover investigations, you can establish a baseline for labor costs. This calculation also highlights potential savings opportunities from implementing proactive, automated, and scaled workflows built on identity intelligence. For instance, if newly discovered credentials and active sessions are automatically flagged for password resets and session re-authentication, the volume of account takeover investigations can be reduced—saving $70 dollars for each incident avoided and unlocking more time for busy analysts to spend on higher value tasks.

[3]Amazon. (2024). Independent sellers keep choosing Amazon for the value we provide. Amazon. https://www.aboutamazon.com/news/small-business/independent-sellers-keep-choosing-amazon-for-the-value-we-provide

Fraud Losses

Losses from fraudulent activity following an account takeover can vary wildly based on the industry and the type of web application involved. For instance, accounts for streaming services typically present lower fraud risks, more or less limited to the value of their monthly subscriptions. In contrast, merchant accounts for e-commerce platforms can result in losses reaching tens of thousands of dollars or more. Below is a chart summarizing estimated per-account fraud losses broken down by industry. While not comprehensive, we intended to illustrate the diverse ways a single compromised account can be exploited for fraudulent activities.

Industry	Per ATO	Fraud Mechanism
Entertainment and Streaming	**$5-$20** Average monthly subscription cost	Resale on illicit markets
Social Media	**$1-$10** For a typical account, higher value accounts can command more money on the dark web	Resale on illicit markets, bots, user to user fraud
Video Games	**$200-$10,000** Variable depending on the game and desirability of the account	Resale on illicit markets, in-game transaction fraud
Cloud Computing/IaaS	**$1000+ per day** Based on cloud computing costs from recent cryptojacking threat reporting[4]	Cryptojacking
Transportation - Airlines	**$500-$2000** Per account based on International Air Transport Association (IATA) fraud estimates[5]	Payment Fraud, Loyalty Point Fraud
Ecommerce	**Highly Variable** Many merchant accounts have been linked to multi-million dollar fraud schemes	Merchant fraud and scams, money laundering

[4]Sysdig. (2024). AMBERSQUID: A new cloud-native cryptojacking operation exploiting AWS services. Sysdig Blog. https://sysdig.com/blog/ambersquid/

[5]Travel Daily News. (2024). How airlines and hotels can address fraud as cyber threats rise. Travel Daily News. https://www.traveldailynews.com/column/featured-articles/how-airlines-and-hotels-can-address-fraud-as-cyber-threats-rise/

Customer Churn Risk

One of the most challenging economic impacts of account takeover (ATO) to quantify is customer churn risk. Regardless of fault, it's reasonable to assume that customers who discover their streaming service, airline account, or social media profile has been compromised are more likely to churn or become inactive than those who have not experienced such an incident. The key question is: how much more likely?

Various studies have attempted to measure the impact of data breaches on customer retention. According to a recent report, 75% of consumers indicated they would consider cutting ties with a brand following a cybersecurity incident[6]. The IBM Cost of a Data Breach Report, a widely referenced industry benchmark, has consistently cited brand and reputation damage as a major contributor to the long-term costs of a breach. In the 2024 report, it was noted that costs related to lost business rose 11% year over year[7]. Since most breaches involve the identity vector, it's reasonable to infer that ATO attacks represent a significant contribution to the overall cost of data breaches, though quantifying their exact impact remains difficult.

A 2023 report from the digital fraud vendor Sift[8] provides a more direct look at customer sentiment toward account takeovers. The study found that:

73%

73% of users believe the brand or company is responsible for preventing ATO attacks and securing account credentials.

43%

Fewer than half (43%) of ATO victims were notified by the company that their account had been compromised.

The Sift report is particularly valuable because it captures both customer sentiment and real-world security experiences, shedding light on how well companies communicate risks and respond to ATO incidents. Using these insights as a baseline, we built a model around Vidz2Stream, a fictional streaming platform with 150 million global users, charging $20 per month ($240 per year) for its service:

ATO Customer Churn Model for Fictional Streaming Platform Viz2Stream

- **Total customers:** 150 million
- **ATO incidence rate:** 0.5%
  - We discussed a 1.4% median ATO exposure rate earlier in the report. Understanding that not all exposures are acted upon by cybercriminals, we're estimating a 0.5% incident rate, roughly 1/3rd of the exposure rate.
- **Implied number of customers impacted by ATO per year:** 750,000
- **Blame the Brand/Company Sentiment:**
  - 73%

[6]Vercara. (2024, February 6). Vercara research: 75% of U.S. consumers would stop purchasing from a brand if it suffered a cyber incident. Vercara. https://vercara.com/news/vercara-research-75-of-u-s-consumers-would-stop-purchasing-from-a-brand-if-it-suffered-a-cyber-incident

[7]IBM. (2024). Cost of a data breach report 2024. IBM. https://www.ibm.com/reports/data-breach

[8]Sift. (2024). Account takeover fraud: Q3 2024 index report. Sift. https://sift.com/index-reports-account-takeover-fraud-q3-2024

- **ATO Notification Split:**
  - Notified by the company (43%): ~322,500
  - Not notified (57%): ~427,500
- **Churn Rate Assumptions:**
  - **Notified + Blame Brand:** 15%
    - Even if they blame the brand, being notified builds some goodwill or at least shows the company took proactive steps. We assume a lower churn than if they were not notified.
  - **Notified + Don't Blame Brand:** 5%
    - This group is relatively more forgiving. They trust that "incidents happen," and the company did the right thing by informing them. A 5% churn rate reflects a smaller fraction that might still quit out of an abundance of caution.
  - **Not Notified + Blame Brand:** 30%
    - This group is likely to feel betrayed because they blame the company and the company failed to notify them. Thus we assume a significantly higher 30% churn rate.
  - **Not Notified + Don't Blame Brand:** 10%
    - Although they don't blame the brand, they still might be upset they weren't informed. Some may leave. We assume a 10% churn rate as a midpoint between minimal discontent (e.g., 5%) and active dissatisfaction (e.g., 30%).
- **Total Assumed Churn:** 145,000 users per year
  - Based on the percentage estimates outlined in Churn Rate assumptions.
- **Revenue Impact:** $34.8 million annually
  - 145,000 churned users multiplied by annual $240 subscription cost

Combining Labor, Fraud, and Customer Churn

To get a holistic understanding of how much ATO and session hijacking costs your business on an annual basis, we can combine all three cost factors. Let's again use the fictional company Vidz2Stream and their profile to add up the costs and quantify the magnitude of this problem:

- **Labor**

  375,000 x 70 = $26.2M

  - Security teams cannot investigate all the incidents they are alerted on due to the ubiquitous problem of "alert fatigue". Various sources put the number around 40-60% investigation[9]. Let's split the difference and assume the Vidz2Stream security team investigates half of their estimated 750,000 ATO incidents.

[9] Chuvakin, A. (2023, October 10). Anton's alert fatigue: The study. Medium. https://medium.com/anton-on-security/antons-alert-fatigue-the-study-0ac0e6f5621c

- **Fraud**

  $20 X 375,000 = $7.5M

  - Let’s assume that the 375K investigations successfully negated any fraud costs related to those accounts.
  - Let’s assume the other 375K resulted in fraud losses equaling the value of 1 month of a Vidz2Stream subscription ($20).
- **Churn**

  $34.8M as calculated in the previous section.

68.5M

In the case of Vidz2Stream, ATO and Session Exposure costs at least $68.5 million dollars annually.

Conclusion

We hope this data provides valuable insights into the scale, impact, and industry trends surrounding exposed sessions. More importantly, we hope it inspires security teams to improve or augment detection and response strategies—shifting toward proactive measures that identify, monitor, and remediate exposed sessions before they can be exploited to head off fraud risks, unlock labor efficiencies, and deliver better security outcomes for end customers.