Arkose Labs

THE ECONOMICS OF ACCOUNT TAKEOVERS: A TIPPING POINT

EBOOK

Cybercriminals may profit by exploiting vulnerabilities, but executing a successful attack against a website demands a certain level of resources and expertise. This type of digital malfeasance comes with its own costs, particularly when the target has robust security measures in place to counter the efforts of bad actors and bots.

At Arkose Labs, we are steadfast in our mission to dismantle the lucrative business model of cybercrime. This informative ebook delves into the intricate economics behind these online attacks and sheds light on the critical tipping point where a threat transitions from a viable endeavor to an unsustainable pursuit. This is the point where the right security solution makes all the difference.

Prepare to unravel the hidden dynamics shaping the realm of account takeover attacks—and learn how your organization can find ongoing, affordable protection amid this evolving landscape.

ACCOUNT TAKEOVER 101

In the realm of cybercrime, attackers exploit websites to generate profit and sustain their illicit livelihood. At its core, this enterprise necessitates that the income derived from these clandestine activities surpasses the associated costs, ideally providing a sustainable lifestyle. Among the most lucrative and prevalent forms of online abuse are account takeover (ATO) attacks. ATOs involve a multi-step process, often including both bots and human scammers.

Numerous studies and reports carried out over time have consistently demonstrated the widespread danger of ATO fraud, affecting both businesses and individuals. Because ATO attacks go hand in hand with identity theft, where a hacker impersonates another to create a new account, this threat now makes up about 36% of the 5.2 million fraud reports the FTC received in 2022 alone.

[1]*https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf*

1. **Data is the greatest target.** When a company falls victim to a breach, it can result in monumental loss of both money and user credentials. Data breaches now occur with alarming frequency—even a single one can encompass hundreds of millions of compromised accounts, as exemplified by the 2021 Facebook breach, which impacted over 500 million users.

2. **Stolen credentials open up even shadier opportunities.** This valuable information is then disseminated on the dark web or public "cybercrime-as-a-service" platforms, available to other attackers either for free or at a nominal fee.

3. **Cybercriminals exploit findings to launch other attacks.** Users often employ the same logins and passwords across multiple platforms, which means bad actors can easily engage in credential stuffing attacks. Here, hackers systematically test stolen credentials against various potential targets, often generating a refined list of valid accounts across different websites.

4. **Attackers profit by selling these packages.** The resulting inventory of confirmed accounts is typically sold as a bundled product on the dark web, consisting of anywhere between 100 to 1,000 accounts. Price varies based on industry. Attackers specializing in ATOs acquire these credentials and employ specific monetization techniques tailored to the targeted websites.

RESEARCH APPROACH AND ASSUMPTIONS

This research aims to analyze attackers specializing in credential stuffing attacks on sites from various industries, with different levels of protection. We'll examine the infrastructure and software they need to deploy for successful attacks against sites protected by a web application firewall (WAF) or an advanced solution like Arkose Bot Manager. Ultimately, we'll determine which solution is most effective in eroding the economic incentive of today's attackers.

This ebook relies on data gathered from the dark web, Telegram, Discord, and other social media platforms, along with insights from the Arkose Labs global network. We made reasonable assumptions regarding the attacker's income, considering their reputation and the likelihood of inventory sales. Additionally, we explored scenarios where the scammer shows persistence in executing successful attacks.

ACHIEVING A WELL-PROTECTED SITE

To enhance site protection, businesses should consider using web application firewalls (WAFs) as a basic layer of defense against common application layer attacks. While WAFs provide elementary bot detection features (such as against DDoS attacks), they may not effectively handle complex and persistent attacks such as credential stuffing or ATOs.

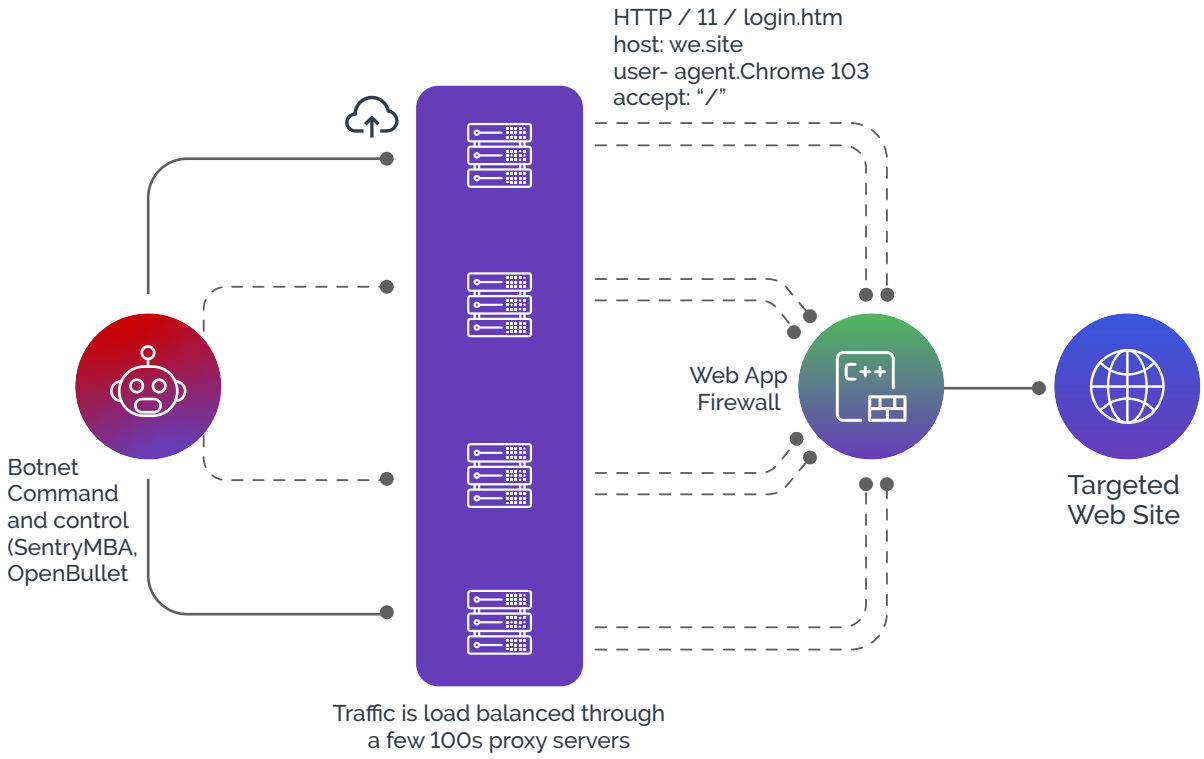
To protect against these dangerous forms of attack, turn to advanced detection and mitigation products like Arkose Bot Manager. This highly effective solution leverages multiple detection methods, including device and IP intelligence, behavioral biometrics, and user behavior anomaly detection, to ensure only human users access critical resources. Bot prevention products go a step further, distinguishing legitimate online traffic from anomalous behavior.

To maximize protection, some website owners develop a comprehensive bot detection layer by integrating signals from various web security products. This multilayered approach ensures a robust defense-in-depth strategy similar to security measures for a physical business location.

SAFEGUARDING A WEBSITE

When a site is poorly protected, criminals don't need to worry about deploying a complex infrastructure for credential stuffing attacks. Instead, they can easily employ a botnet with a limited number of nodes, using off-the-shelf tools like Sentry MBA or OpenBullet. The main concern is throttling the request flow to avoid overwhelming the target website. Sometimes, this poorly calibrated attack may unintentionally lead to denial of service and prolong the verification process for a large set of credentials.

In this simplified scenario, the botnet could consist of just one machine, such as a laptop running a Sentry MBA script and distributing requests through cheap proxies in data centers. It's worth remembering, this uncomplicated setup can bypass basic WAF settings.

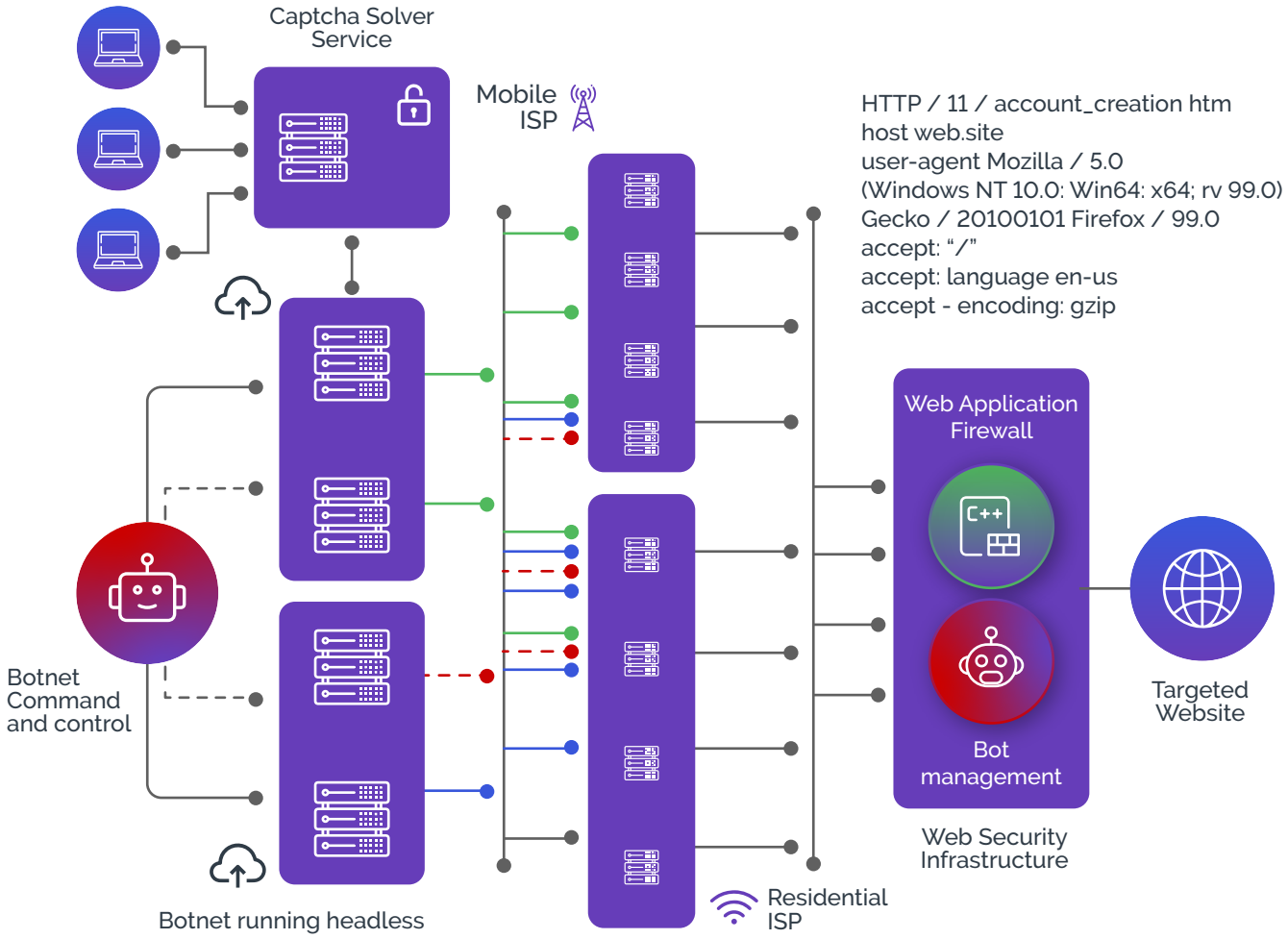


Example of simple automated attack

With the advanced capabilities of Arkose Bot Manager in place, attackers need increased sophistication to evade detection. Attackers need to update their strategy to include additional resources such as:

- Spreading traffic through a vast botnet of over 10,000 nodes across multiple continents
- Masking the traffic's origin to appear as residential and mobile ISPs rather than data centers to avoid suspicion
- Mimicking legitimate user behavior, following similar workflows to access resources
- Sending expected data and ensuring variety in the fingerprint to avoid detection based on client-side characteristics
- Dealing with a significant portion of the attack traffic being blocked or challenged, necessitating resubmissions and lengthening the attack process

The infrastructure for such attacks may involve a laptop orchestrating virtual machines in a cloud infrastructure, generating traffic through residential and mobile proxies. The software used can range from advanced Python scripts to headless browsers that mimic complex user behaviors. Additionally, the botnet must employ CAPTCHA solver services—using AI or low-cost human workers—to overcome challenges like those presented by Arkose MatchKey.



Deployment with Arkose Bot Manager

FACTORS AFFECTING THE REVENUE POTENTIAL

Before delving into the cost, let's evaluate the factors that will affect the revenue potential for attackers.

Hit Rate

This metric determines the number of valid sets of credentials harvested from the credential stuffing attack. The ratio can vary based on the industry and the quality of the combo list, which contains known username and password combinations.

INDUSTRY	REASONING
Financial Services | Banking | Fintech | Insurance	Financial services websites often don't use email addresses as user IDs, which affects the hit rate. Users are also more cautious about reusing credentials from other sites for their bank login. As a result, an expected hit rate of 10% is anticipated.
eCommerce | Retail	eCommerce websites typically have an estimated hit rate of about 15% since using email addresses as user IDs is widespread. Additionally, finding combo lists containing email addresses and passwords is much easier in these cases.
Travel | Hospitality	Travel and hospitality websites typically have an estimated hit rate of about 15%, for many of the same reasons as ecommerce and retail sites.
High Tech | Media | P2P Marketplaces	Like ecommerce and travel sites, high-tech, social media, and marketplaces commonly use email addresses as login credentials. As such, estimated rates of 15% are typical.
Gaming	Gaming sites have two types of accounts: premium and lower-value. Due to their young user community, bulk accounts have an expected hit rate of no more than 5%. For premium accounts, the chances of being harvested are considerably lower, not exceeding 0.0075%. Premium accounts are high-value, offering valuable in-game assets like powerful weapons or sports cars, making them attractive on the dark web. On the other hand, lower-value accounts are sold in bulk, offering unknown or limited assets.

Based on an average quality combo list with 1 million credentials, the following table presents the estimated total number of harvested credentials from the credential stuffing attack per industry.

Gaming	Estimated Hit Rate	Estimated credential harvested
eCommerce, Social Media	15%	150,000
Fintech/Banking	10%	100,000
Gaming - Bulk accounts	5%	50,000
Gaming - Premium accounts	0.0075%	75

ATTACKER'S REPUTATION

The dark web serves as a marketplace for both legitimate and fraudulent goods and services. Criminals exploit these platforms to sell private information obtained from credential stuffing attacks. A reseller's reputation directly influences the percentage of their inventory that gets acquired. New resellers with no or low reputation may sell up to 20% of their inventory, medium-reputation resellers may find up to 40%, and highly reputable resellers may earn at least 60% of their inventory.

ACCOUNT MARKET PRICE

The market price of a user's credential varies by industry. The table below shows the current market price and potential revenue of various types of accounts by industry based on the estimated credential harvested after completing an attack. Gaming credentials offer the largest revenue potential followed by fintech/bank credentials.

Industry	Average revenue / Credential	Good Reputation	Medium Reputation	Bad Reputation
e-Commerce	$0.08	$7,200.00	$4,800.00	$2,400.00
Social media	$0.10	$9,000.00	$6,000.00	$3,000.00
Fintech / Bank	$0.40	$24,000.00	$16,000.00	$8,000.00
Gaming - Bulk Accounts	$1.70	$51,000.00	$34,000.00	$17,000.00
Gaming - Premium accounts	$648	$29,160.00	$19,440.00	$9,720.00

PERFORMANCE OF THE WEB SECURITY PRODUCT AND THE TEAM THAT PROTECTS A SITE

The performance of the web security product and the team that protects the site will bring some level of uncertainty for the attacker, and the least patient or least skilled will most likely give up their attack before it completes—and move on to an easier target. At times, the most effective security products are likely to block or challenge close to 100% of the attack traffic, increasing the need for the attacker to resubmit requests. This move extends the timeline to completion, and in some cases the cost of the attack.

Frequent software updates are essential for adjusting the botnet's attack strategy to overcome existing defenses. Certain updates may require extensive testing and development, spanning days or weeks. Some attackers may ultimately abandon their attack

if they can't overcome the defense in place. Both defenders and attackers feel the pressure to stay vigilant. Below is an estimated time for completing a credential stuffing attack with one million credentials, considering attack velocity and assuming no downtime due to software updates necessitated by a strong defense strategy protecting user identities.

Humans can be impatient and often prefer to execute attacks quickly by sending requests at a high velocity. However, this approach has drawbacks. It makes the attack more noticeable to defenders and increases the total number of requests needed to succeed. For sites protected with a web application firewall, attackers are better off adopting a low attack velocity to stay unnoticed and minimize the number of replays required. By doing so, the attack can be completed within approximately two and a half days.

Attack Velocity	Requests / hour	Replay Factor	Total Requests	Est. days to complete
Low	25,000	1.5	1,500,000	2.50
Medium	50,000	3	3,000,000	2.50
High	150,000	6	6,000,000	1.67

Websites that use a bot management solution are more effective in identifying attacks conducted at a lower velocity, leading to a higher replay factor when compared to using a WAF solution. When the attack velocity is increased, the machine-learning models in bot and fraud detection products perform better, enabling them to identify and block or challenge the attack pattern. Consequently, this leads to a significant increase in the replay factor and extends the time needed to complete the attack, even when sending traffic at a high velocity, to nearly 3 days.

Attack Velocity	Requests / hour	Replay Factor	Total Requests	Est. days to complete
Low	25,000	1.9	1,900,000	3.17
Medium	50,000	4	4,000,000	3.33
High	150,000	10	10,000,000	2.78

Arkose Bot Manager's challenge strategy effectively hinders attack speed by countering traditional CAPTCHA solver services, which can be limited in staffing capacity. If, for instance, a CAPTCHA solver worker can handle three CAPTCHAs per minute and about 100 workers are assigned to solve the attack's challenges, the attackers can achieve a maximum request rate of 18,000 requests per hour. However, this approach also amplifies the replay factor,

considering potential solver errors and time constraints. Consequently, the attack completion time may triple.

Requests / hour	Replay Factor	Total Requests	Est. days to complete
18,000	4	4,000,000	9.26

When attacking a well-protected site, the number of replays, the lack of fast progress, the complexity of the attack strategy, the rising cost, and the uncertainty of how long the attack will take to complete may unnerve less experienced attackers and convince them to give up early, significantly affecting their inventory and ultimately their net income.

WHAT DOES IT TAKE TO DEFEAT A WELL-PROTECTED SITE?

ATTACKING A SITE PROTECTED WITH A WEB APPLICATION FIREWALL

As discussed earlier, the infrastructure needed for a successful attack varies based on the protection a company has in place. A website protected with a WAF solution will only require a basic shared data center-hosted proxy service to defeat the rate limiting in place. The average cost for such service at the time of this writing is $52 per month.

Number of sites attacked	1	2	3	4	5
Proxy Cost (Monthly)	$52	$52	$52	$52	$52
Total Cost (Yearly)	$624	$624	$624	$624	$624

ATTACKING A SITE PROTECTED WITH A BOT MANAGEMENT PRODUCT

For sites protected with more advanced bot management solutions or Arkose Bot Manager, the attacker's use of a basic proxy service will not be sufficient. A more costly proxy service leveraging mobile and residential ISP IP addresses is required. The average cost for this type of proxy service with the ability to load-balance the traffic through over 100,000 IP addresses is currently $700 per month. The attacker will also need to host the command and control center in the cloud. Compute and storage are cheap, and a single server per site attacked will amount to about $50 per month.

Number of sites attacked	1	2	3	4	5
Hosting and Storage cost (Monthly)	$50	$100	$150	$200	$250
Proxy Cost (Monthly)	$700	$700	$700	$700	$700
Total Cost (Monthly)	$750	$800	$850	$900	$950
Total Cost (Yearly)	$9000	$9600	$10,200	$10,800	$11,400

ATTACKING A SITE PROTECTED WITH ARKOSE BOT MANAGER

Websites protected with an advanced bot management solution that includes dynamic challenge capabilities like Arkose Bot Manager will require attackers to double the hosting cost per site they attack to manage the more complex workflow of solving the challenge. It will additionally require the attacker to integrate the botnet with a puzzle-solving service. The average cost at this time is $2.12 per 1,000 requests. The limited bandwidth will significantly increase the time it takes to complete the credential stuffing attack and, because of the duration, make it more noticeable and give the defender plenty of opportunities to mitigate it, thus increasing the number of retries necessary.

For this simulation, let's consider that a credential needs to be submitted to the puzzle-solving service four times before it is successfully validated. In this case, it will require about 4 million requests to validate 1 million credentials. The table below summarizes the total cost based on the number of sites attacked.

Number of sites attacked	1	2	3	4	5
CAPTCHA Solver cost	$8,480	$16,960	$25,440	$33,920	$42,400
Hosting and storage cost (monthly)	$100	$200	$300	$400	$500
Proxy Cost (Monthly)	$700	$700	$700	$700	$700
Total Cost (Monthly)	$9,280	$17,860	$26,440	$35,020	$43,600
Proxy Cost (Monthly)	$18,080	$27,760	$37,440	$47,120	$56,800

It's worth noting, many CAPTCHA solvers will not even attempt to tackle the puzzle challenges of Arkose MatchKey. The time it takes to solve them is too costly for attackers, and the effort cannot be effectively automated.

THE ATTACKER'S NET INCOME

Making a good income is typically what motivates anyone to do any sort of work. Now that we have a good understanding of the potential revenue and cost of attacking a website, let's see if the business of cybercrime is more lucrative than finding another type of job, based on the level of protection in place on the targeted website.

NET INCOME AGAINST A SITE PROTECTED WITH WAF

Let's first consider a site protected with a WAF solution with some basic bot management rules and rate limiting. As one can see in this case, an attacker can make some money from Day One even if they are starting with no experience. Considering the low level of skill, infrastructure, and maintenance required to carry out the attack, it may be done as a hobby or even a side hustle for additional income. This may potentially attract a lot of "script kiddies" who are looking to make a few bucks.

Note: When considering the typical resell price of fintech, banking, and gaming accounts, the revenue potential appears to be significantly higher. However, it's essential to acknowledge that finding poorly protected sites may be quite uncommon. As a result, the six-figure high revenue potential mentioned here remains largely theoretical.

Number of sites	1	2	3	4	5
Total Cost (Yearly)	$624	$624	$624	$624	$624
Income - eCommerce					
Low Reputation	$1,776	$4,176	$6,576	$8,976	$11,376
Medium Reputation	$4,176	$8,976	$13,776	$18,576	$23,376
High Reputation	$6,576	$13,776	$20,976	$28,176	$35,376
Income - Social Media					
Low Reputation	$2,376	$5,376	$8,376	$11,376	$14,376
Medium Reputation	$5,376	$11,376	$17,376	$23,376	$29,376
High Reputation	$8,376	$17,376	$26,376	$35,376	$44,376
Income - Fintech/Banking					
Low Reputation	$7,376	$15,376	$23,376	$31,376	$39,376
Medium Reputation	$15,376	$31,376	$47,376	$63,376	$79,376
High Reputation	$23,376	$47,376	$71,376	$95,376	$119,376
Income - Gaming - Bulk accounts					
Low Reputation	$16,376	$33,376	$50,376	$67,376	$84,376
Medium Reputation	$33,376	$67,376	$101,376	$133,376	$169,376
High Reputation	$50,376	$101,376	$152,376	$203,376	$254,376
Income - Gaming - Premium accounts					
Low Reputation	$9,096	$18,816	$28,536	$38,256	$47,976
Medium Reputation	$18,816	$38,256	$57,696	$77,136	$96,576
High Reputation	$28,536	$57,696	$86,856	$116,016	$145,176

NET INCOME AGAINST A SITE PROTECTED WITH A BOT MANAGEMENT PRODUCT

A site protected by a solution like Arkose Bot Manager changes things for attackers. Those with no skills will quickly be discouraged and go out of business. Considering the time investment to set up the infrastructure and build and maintain the software, the attacker will need to target more than one site to make the whole operation viable.

Even an attacker with a good reputation reselling on the dark web and targeting multiple e-commerce and social media sites will make a fairly low annual salary (between $24K and $34K), which is in the ballpark of what a mid-level software engineer will make in a major city in countries like Russia, India, Colombia, or Argentina. But it would still be much lower for developers located in Thailand or China. Attackers targeting fintech and the gaming industry, however, will make much better money, with the possibility of earning a six-figure income for a highly skilled attacker with a very good reputation.

Number of sites	1	2	3	4	5
Total Cost (Yearly)	$9000	$9600	$10,200	$10,800	$11,400
Income - eCommerce					
Low Reputation	-$6,600	-$4,800	-$3,000	-$1,200	$600
Medium Reputation	-$4,200	$0	$4,200	$8,400	$12,600
High Reputation	-$1,800	$4,800	$11,400	$18,000	$24,600
Income - Social Media					
Low Reputation	-$6,000	-$3,600	-$1,200	$1,200	$3,600
Medium Reputation	-$3,000	$2,400	$7,800	$13,200	$18,600
High Reputation	$0	$8,400	$16,800	$25,200	$33,600
Income - Fintech/Banking					
Low Reputation	-$1,000	$6,400	$13,800	$21,200	$28,600
Medium Reputation	$7,000	$22,400	$37,800	$53,200	$68,600
High Reputation	$15,000	$38,400	$61,800	$85,200	$108,600
Income - Gaming - Bulk accounts					
Low Reputation	$8,000	$24,400	$40,800	$57,200	$73,600
Medium Reputation	$25,000	$58,400	$91,800	$125,200	$158,600
High Reputation	$42,000	$92,400	$142,800	$193,200	$243,600
Income - Gaming - Premium accounts					
Low Reputation	$720	$9,840	$18,960	$28,080	$37,200
Medium Reputation	$10,440	$29,280	$48,120	$66,960	$85,800
High Reputation	$20,160	$48,720	$77,280	$105,840	$134,400

NET INCOME AGAINST A SITE PROTECTED WITH ARKOSE BOT MANAGER

Now, let's consider the possible net income for sites protected with Arkose Bot Manager. What makes a huge difference here is the cost of the puzzle-solver service that is required, which, considering the volume of requests needed to complete the attack, can go into the tens of thousands of dollars. In fact, for ecommerce and social media sites, the loss increases with the number of sites attacked, bankrupting the attacker in no time.

For attackers targeting financial services and banks, the situation appears more favorable to experienced attackers with a good reputation. But when we consider the annual revenue, allowing for the effort required to successfully attack and resell the inventory for at least four websites, it is much easier to earn a living as a regular software developer. Attackers targeting gaming companies fare better. The ones with experience and a good reputation will be able to achieve a comfortable income (over six figures for the experts who target multiple sites). But in contrast, a new entrant in the field would be better off finding a job as a software developer in a reputable company.

Number of sites	1	2	3	4	5
Total Cost (Yearly)	$18,080	$27,760	$37,440	$47,120	$56,800
Income - eCommerce					
Low Reputation	-$15,680	-$22,960	-$30,240	-$37,520	-$44,800
Medium Reputation	-$13,280	-$18,160	-$23,040	-$27,920	-$32,800
High Reputation	-$10,880	-$13,360	-$15,840	-$18,320	-$20,800
Income - Social Media					
Low Reputation	-$15,080	-$21,760	-$28,440	-$35,120	-$41,800
Medium Reputation	-$12,080	-$15,760	-$19,440	-$23,120	-$26,800
High Reputation	-$9,080	-$9,760	-$10,440	-$11,120	-$11,800
Income - Fintech/Banking					
Low Reputation	-$10,080	-$11,760	-$13,440	-$15,120	-$16,800
Medium Reputation	-$2,080	$4,240	$10,560	$16,880	$23,200
High Reputation	$5,920	$20,240	$34,560	$48,880	$63,200
Income - Gaming - Bulk accounts					
Low Reputation	-$1,080	$6,240	$13,560	$20,880	$28,200
Medium Reputation	$15,920	$40,240	$64,560	$88,880	$113,200
High Reputation	$32,920	$74,240	$115,560	$156,880	$198,200
Income - Gaming - Premium accounts					
Low Reputation	-$8,360	-$8,320	-$8,280	-$8,240	-$8,200
Medium Reputation	$1,360	$11,120	$20,880	$30,640	$40,400
High Reputation	$11,080	$30,560	$50,040	$69,520	$89,000

ATTACKER'S NET INCOME VS. SOFTWARE DEVELOPER INCOME BY COUNTRY

Some of the income estimates from the above simulation may seem low for legitimate salaries in wealthier countries. But in some parts of the world, these low incomes may be higher than what a mid-level software developer may expect while working for a legitimate company. For example, an attack against ecommerce or social media websites protected with a solution like Arkose Bot Manager is still highly profitable for someone who lives in Venezuela, Belarus, Cambodia, Tunisia, El Salvador, Ukraine, or Macedonia.

But an attacker located in the Philippines, Kenya, Guatemala, or Vietnam would most likely target a fintech, banking, or gaming site to make their cybercrime efforts more profitable than working a legitimate job. (Source: https://teleport.org/).

Country (City)	Media software developer annual income
Venezuela (Caracas)	$1932
Belarus (Minsk)	$4800
Cambodia (Phnom Penh)	$6696
Tunisia (Tunis)	$7248
El Salvador (San Salvador)	$8484
Ukraine (Kyiv)	$10,644
Macedonia (Skopje)	$14,280
Philippines (Manila)	$16.188
Kenia (Nairobi)	$16,848
Guatermata (Guatemala City)	$21.264
Malaysia (Kuala Lumpur)	$21,324
Vietnam (Ho Chi Minh)	$23,040
Indonesia (Jakarta)	$24,372
Russia (Moscow)	$25,452
India (Mumbai)	$25,920
Colombia (Bogota)	$30.840
Thailand (Bangkok)	$36,972
China (Beijing)	$49,356

CONCLUSION

The motivating intention of this paper was to reveal for the first time the economics behind one of the most lucrative types of online attacks fraudsters perpetrate—ATOs. This was a worthy endeavor because to bankrupt the business model of fraud, it is critical first to understand the underlying economics of fraud. After deep research and analysis, this ebook clearly outlines how ATOs happen, the factors that influence whether an attack will generate net income for a cybercriminal, and how various types of defenses drive up the attacker's cost.

Experienced attackers with strong reputations on the dark web can still make decent revenue, while new entrants struggle to start and earn enough. When comparing different levels of web security solutions, some defenses significantly raise the attackers' costs and diminish their potential earnings. This encourages them to either halt their activities or target less protected entities. Additionally, the paper sheds light on a crucial aspect of ATO: the time-factor for an attack. It answers the question of how long an attack will take, based on a company's defense controls. If the attack is too time-consuming, it becomes unprofitable, prompting the attacker to move on to easier targets.

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M credential stuffing and SMS toll fraud warranties. Its AI-powered platform combines powerful risk assessments with dynamic attack response to undermine the strategy of attack, all the while improving good user throughput. Headquartered in San Mateo, CA with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Arkose Labs

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as the 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M warranties for credential stuffing and SMS toll fraud. With 20% of our customers being Fortune 500 companies, our AI-powered platform combines powerful risk assessments with dynamic threat response to undermine the strategy of attack, all while improving good user throughput. Headquartered in San Mateo, CA, with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 400 Concar Dr, San Mateo, CA 94402

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

Schedule Demo