Threat Vector Dossier: Gaming Industry

Covert Monetization of Skill and Exploits in Gaming Economies

Overview

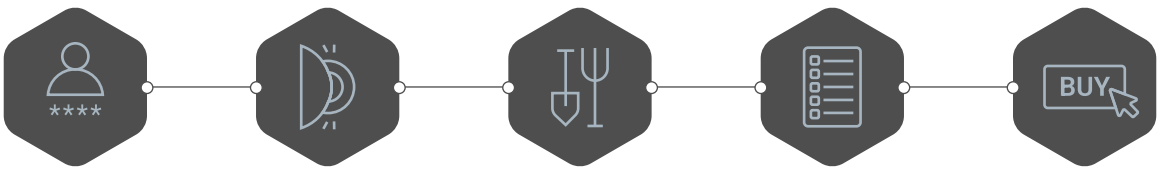
The online gaming industry faces a sophisticated threat from opportunistic actors exploiting economic incentives across the global gaming ecosystem. These operators run large-scale monetization schemes through fake account creation, manual account leveling and gray market resales—violating terms of service while siphoning millions from publishers. Unlike traditional cybercriminals, they employ "low and slow" tactics, manually grinding through game content to build valuable assets for resale on gray markets where accounts sell for 10-25x their initial cost. This illicit activity is part of a global real-money trading ecosystem valued at $19.4 billion annually,[1] with impacts including undermined competitive integrity and inflated in-game economies.

> "It's not bored kids playing games in their spare time. It's highly skilled players reselling valued titles and inventory for profit."
> **- ACTIR threat researcher**

The Fraud Framework

The Arkose Cyber Threat Intelligence Research (ACTIR) unit has uncovered a complex threat landscape where actors with varying motivations and sophistication levels exploit gaming economies. These operators represent a broad spectrum—some might be skilled players cashing in on their abilities, others could be organized fraudsters. What unites them is their human-driven approach, leveraging skill, time and volume to generate illicit profits. They operate in the murky space between legitimate gameplay and commercial exploitation, often working across multiple time zones and regions to maximize profits from their gaming expertise.

These actors manually create accounts with faux sign-up credentials, then invest extensive time grinding through game content to accumulate valuable assets and collect rare items. Many supplement their operations through account takeovers (ATOs), stealing high-value accounts from legitimate players. The human element makes this threat particularly difficult to detect and combat.



[1] https://www.businessresearchinsights.com/market-reports/real-money-skill-games-market-105656

The consequences for gaming studios are severe. Publishers face not only direct revenue displacement but also the erosion of their carefully balanced game economies and the devaluation of legitimate player achievements. What makes this threat particularly pernicious is its human-driven nature—masses of skilled players working to exploit gaming systems without their behavior getting flagged. This represents a fundamental challenge to the gaming industry's economic model, requiring innovative detection and enforcement strategies.

Threat Actor Profile

Category	Description
Type	Economic abuse actor
Motivation	Profit
Skills	High gaming skill, marketplace knowledge
Special tools used	None (manual labor or basic marketplace tools)
Infrastructure	Gray-market platforms (forums, resale sites)
Geography	Global (activity spans multiple servers/regions)

Threat Actor TTPs (Tactics, Techniques, Procedures)

Tactic 1: Mass Creation of Legitimate-Looking Accounts (Initial Access)

Technique:
Actors purchase licenses for games using fake or burner accounts—sometimes dozens per person.

Procedure:
These accounts are manually played, often for long hours, to accumulate rare items, earn in-game currency or reach high levels.

Tactic 2: Manual Grinding for Profit (Exploitation & Monetization)

Technique:
Skilled gamers "grind" through game content rapidly and efficiently.

Procedure:
Once maxed out or loaded with desirable items, the accounts are sold through gray market sites, with prices often ranging from $100 to $2,500 depending on the value of the inventory.

Tactic 3: Gray Market Item and Currency Resale (Persistence)

Technique:
In-game currency and rare items are acquired cheaply and sold on unauthorized marketplaces.

Procedure:
One example showed 45 million currency units being sold for $25—far cheaper than legitimate rates.

Tactic 4: Low-and-Slow Farming (Operational Stealth)

Technique:
No bots, no scripts—just persistence.

Procedure:
Accounts are created and leveled over time to avoid detection. Actors limit automation to avoid triggering fraud detection or anti-bot protections.

Tactic 5: Phishing for ATOs (Account Takeover, Limited Use)

Technique:
Phishing scams targeting active players to steal high-value accounts.

Procedure:
Limited in scale, these ATOs allow actors to resell accounts without manual labor.

Gray Market Seller Spotlight: Inside a Major Operation

To understand the scale and sophistication of gray market operations, ACTIR examined one of the largest sellers operating across multiple platforms. This seller exemplifies how these operations have evolved from small-scale hustles into significant commercial enterprises.

Operation Profile:

Scale: Estimated 75,000-100,000 total account sales over 7+ years

Revenue: Approximately $5 million in total revenue generated

Price Range: Gaming accounts sold from $5 to $1,790

Average Transaction: ~$50 per sale

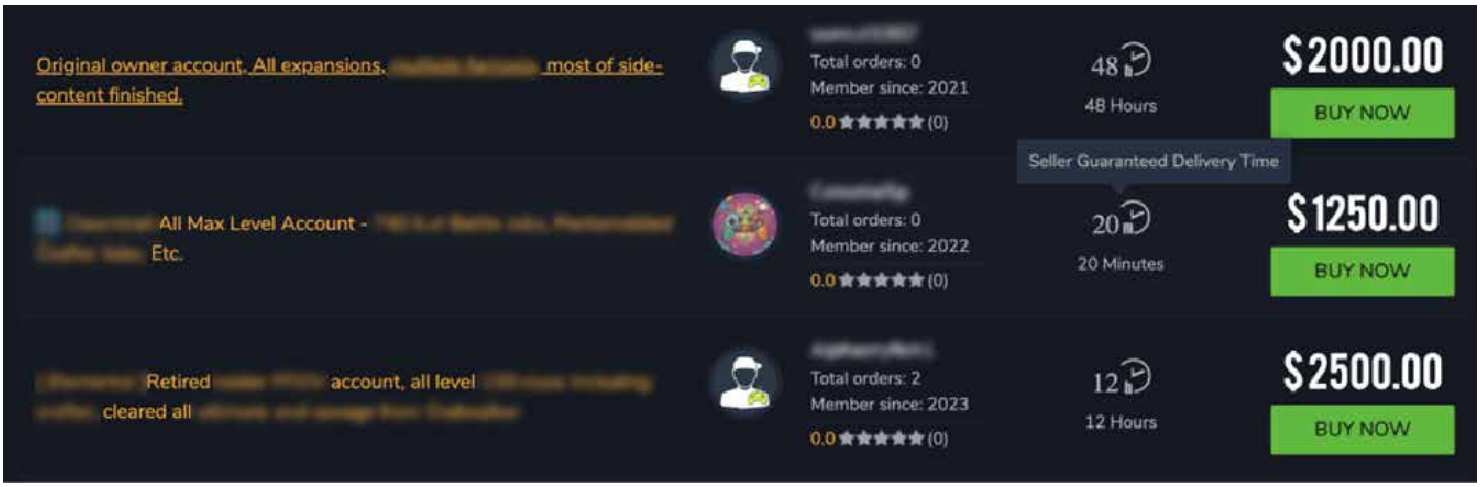
Platform Coverage: Multiple major gaming titles and marketplaces

Customer Base: Global reach with concentrated activity in North America and Europe

This operation demonstrates several key characteristics of sophisticated gray market sellers:

- **Diversified Inventory:** Maintain accounts across dozens of game titles to reduce dependency on any single publisher
- **Professional Presentation:** Use legitimate-looking storefronts and customer service systems
- **Volume Operations:** Process hundreds of transactions monthly with streamlined delivery systems
- **Platform Strategy:** These third-party platforms are not actually selling anything, but rather facilitating transactions between individuals

The longevity of this operation—surviving over 7 years in the market—highlights the challenge publishers face in combating these sellers. Their ability to generate millions in revenue from activities that are generally against the End User License Agreement (EULA) or Terms of Service (ToS) of most games underscores the economic incentives driving this ecosystem.



Economic Impact

The economic damage from “low and slow” attacks creates cascading effects throughout gaming ecosystems. These human-driven operations are particularly challenging because they don't use bots or automation—making them nearly impossible to distinguish from legitimate players.

Direct Revenue Displacement

- Players bypass initial game purchases and months of in-game spending by buying pre-leveled accounts.
- Lost revenue opportunities arise when a player purchases virtual items and currency on the gray market instead of from the publisher itself.
- Gray market currency sales undercut official pricing by 80-90%, devaluing publisher monetization.

Game Economy Disruption

- Armies of manual farmers grinding 16+ hours daily flood markets with currency and rare items.
- Legitimate players' achievements lose value when maxed accounts sell for a fraction of the time investment required.
- In-game economies suffer inflation as manually farmed resources saturate marketplaces.

In addition, there are hidden operational costs. Publishers must invest heavily in behavioral detection systems, economic rebalancing efforts and expanded customer support—all to combat actors who appear indistinguishable from legitimate players during gameplay.

Recommendations

Combating this problem requires a multi-layered approach that balances security measures with legitimate player experience. Since these actors employ human skill rather than automation, traditional anti-bot defenses prove ineffective. Publishers must instead focus on behavioral analytics, economic controls and strategic enforcement to protect their ecosystems without alienating genuine players.

1. **Detect Multi-Account Behavior Patterns**
   Monitor for users creating multiple game licenses from a single IP, region or device type.
2. **Enforce Stronger In-Game Account Linking**
   Tie progress and purchases to identity elements like phone verification or hardware binding.
3. **Flag High-Velocity Level Completions**
   Use behavioral analytics to spot accounts that complete full games within unnatural timeframes.
4. **Watermark and Trace In-Game Currency**
   Introduce traceability to detect in-game currency laundering or illegitimate exchanges.
5. **Monitor and Takedown Gray Market Listings**
   Actively crawl resale marketplaces to identify and take down unauthorized sales.

Looking Ahead: The Agentic AI Risk

While the operation is currently manual and human-driven, concerns loom about future threats from agentic AI models trained to play and level in-game accounts. These systems would reduce operational labor, increase scale and deepen fraud risks—especially if powered by reinforcement learning.

> If attackers start using Agentic AI to automate play, this fraud model scales dramatically. It would be catastrophic for fair play and publisher revenue."
> **- ACTIR threat researcher**

However, current GPU and resource costs make this impractical today.

Conclusion

This fraud ecosystem is a shape-shifting, hard-to-pin-down adversary in the world of digital gaming fraud. What makes it dangerous is the legitimate veneer—it's not malware, not bots and not brute-force attacks. It's skill, time and business acumen applied toward gaming ecosystems in ways developers never intended.

The challenge is cultural as well as technological. Without decisive intervention, this blend of gray-market legitimacy and black-hat monetization will continue to siphon value from publishers, degrade player experience and normalize a shadow economy.

About ACTIR

Arkose Cyber Threat Intelligence Research (ACTIR) unit is a dedicated and specialized counterintelligence team embedded in Arkose Labs. Composed of full-time experts in cyber threat analysis, digital forensics and cybersecurity operations, ACTIR's primary mission is to identify, assess and neutralize sophisticated cyber threats. By leveraging cutting-edge technologies and methodologies, ACTIR provides actionable intelligence and orchestrates coordinated responses to mitigate threats. Recently it partnered with Microsoft DCU and law enforcement to disrupt Vietnamese threat actor group Storm-1152. Through collaboration with Arkose Lab's award-winning SOC, ACTIR plays a pivotal role in enhancing the cybersecurity posture and ensuring the integrity of the digital infrastructure of Fortune 500, category-leading enterprises and trailblazing businesses.
Access ACTIR's threat research taxonomy.

Contact ACTIR to discuss these insights: actir@arkoselabs.com

Cassie Stevenson
Arkose Labs
Director of Brand and Communications
c.stevenson@arkoselabs.com