



Hospitality Sector **Deep Dive**

How Threat Actors Turn Vulnerabilities Into Big Business

Contents

Overview	4
Hotel and Restaurant Fraud	6
What Hackers Can Do with Deep Access	8
Fraudsters Study and Share Booking Platform Secrets	10
Cooperative Fraud	12
Dark Web Travel Agents	14
Casino Fraud	17
Some Casino Fraud Schemes Shared on the Dark Web	17
Security Recommendations for Hospitality Businesses	20

Overview

The hospitality industry as we know it may be deeply invested in digital transformation to keep up with consumers' preferences and expectations of a seamless experience from booking to the experience itself. But so are threat actors. SpiderLabs' research has found that fraudsters are professionalizing and cooperating at the same pace as their counterparts on the legitimate side of the industry.

So much so, in fact, that SpiderLabs has found illicit bookings platforms on the dark web that use stolen payment details and vulnerabilities on popular booking platforms to sell heavily discounted bookings and services.

This professionalization goes hand-in-hand with a surprising level of cooperation and knowledge-sharing on best practices to attack hospitality organizations. SpiderLabs even uncovered evidence of casino fraud schemes that offer to set-up entire illicit casino operations.

Hospitality is a big business, and unfortunately so are the vulnerabilities in organizations' networks. Read on to learn how threat actors are monetizing these vulnerabilities.

This report is part of the [2025 Trustwave Risk Radar Report: Hospitality Sector](#), a comprehensive report that provides a deeper and broader understanding of the risks and threats that affect the hospitality industry.

The hospitality industry has heavily invested in digital transformation efforts to keep up with ever-changing customer preferences and demands and make operations more efficient. Digital transformation and hyper-personalization are now top priorities in the hospitality industry as organizations race to keep pace with customer expectations while trying to drive operational efficiency.

Unfortunately, threat actors are also investing deeply and professionalizing with more nefarious goals in mind. Today's cybercriminals are operating in a more organized and collaborative manner, sharing their knowledge on dark web forums and working together to carry out a plethora of fraudulent schemes, including chargeback scams, loyalty account takeovers, supplier invoice fraud, and even money laundering.

The Trustwave SpiderLabs team created this report to provide insight into how malicious actors can wreak havoc on hospitality businesses once they gain unauthorized access to their networks, the concerning collaborative efforts among cybercriminals that perpetuate complex fraud schemes, underground "travel agencies" that offer too-good-to-be-true travel deals, and casino fraud schemes.

This report also looks at dark web travel agencies and how the cybercriminal economy has evolved to become more professional and diverse in its offerings and provides helpful security recommendations to help hospitality businesses thwart novel and sophisticated fraud schemes. This report is part of the 2025 Trustwave Risk Radar Report - Hospitality Sector a comprehensive report that provides a deeper and broader understanding of the risks and threats that affect the hospitality industry.

Hotel and Restaurant Fraud

The hospitality industry — particularly hotels and restaurants — has become an increasingly attractive target for fraudsters due to its unique combination of high-volume transactions, sensitive customer data, decentralized operations, and often under-resourced cybersecurity practices. These businesses manage a steady flow of personal and financial information, including payment card data, identity documents, booking histories, loyalty accounts, and even travel itineraries. At the same time, they face constant operational pressure to deliver fast, seamless guest experiences that can sometimes lead to weaker security enforcement at the point of service. This intersection of convenience, value, and vulnerability creates ideal conditions for a wide spectrum of fraud tactics to thrive.

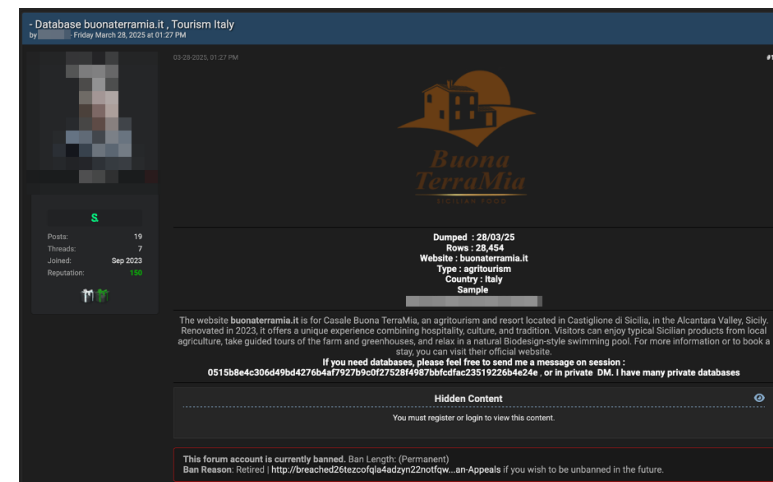


Figure 1. A database of a hospitality business being advertised on the dark web

Hotels are especially lucrative for cybercriminals because of the rich data they store and the trust customers place in their systems. A single breach of a hotel's property management system (PMS) or online booking platform can expose thousands — or even millions — of records containing names, email addresses, phone numbers, passport scans, payment data, and VIP status indicators. Once stolen, these databases become powerful tools for fraud. Attackers often use them to craft convincing phishing emails posing as hotel staff or payment processors, targeting past guests with fake invoices or refund scams. In some cases, the data is sold in bulk on the dark web to other criminal groups, who then use it for identity theft, credential stuffing, or financial fraud.

What Hackers Can Do with Deep Access

When attackers gain high-level access to hospitality networks — particularly through domain administrator accounts or third-party cloud platforms such as AnyDesk, TeamViewer, or Azure AD — the potential for fraud escalates from isolated theft to full-scale, coordinated exploitation. These scenarios move beyond data breaches into active manipulation of systems, finances, and customer interactions.

If a cybercriminal obtains domain admin access within a hotel or restaurant's internal network, they effectively control the digital infrastructure. With this access, an attacker can impersonate any employee, reset passwords, and bypass access restrictions across all connected systems. From a fraud perspective, this opens multiple paths. The attacker could modify reservation records, generate fake refunds to accounts under their control, or alter financial reports to mask stolen funds. They might access point of sale (POS) systems and property management systems (PMS) to extract payment data or reroute transactions through fraudulent payment processors. More subtly, they could place ghost employees on the payroll, reroute loyalty point redemptions, or even manipulate supplier invoicing for kickbacks. All of this can be done while maintaining the illusion of normal operations — making detection slow and forensic tracing difficult.

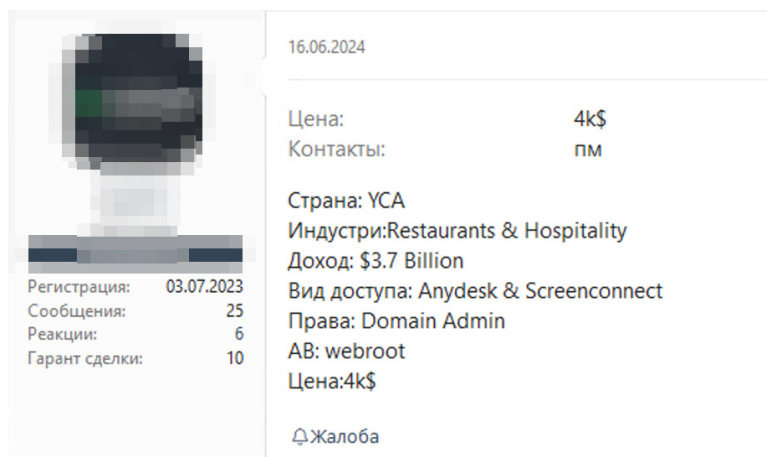


Figure 2. Actor offers remote monitoring and management (RMM) access with domain admin rights to a US-based restaurant and hospitality facility

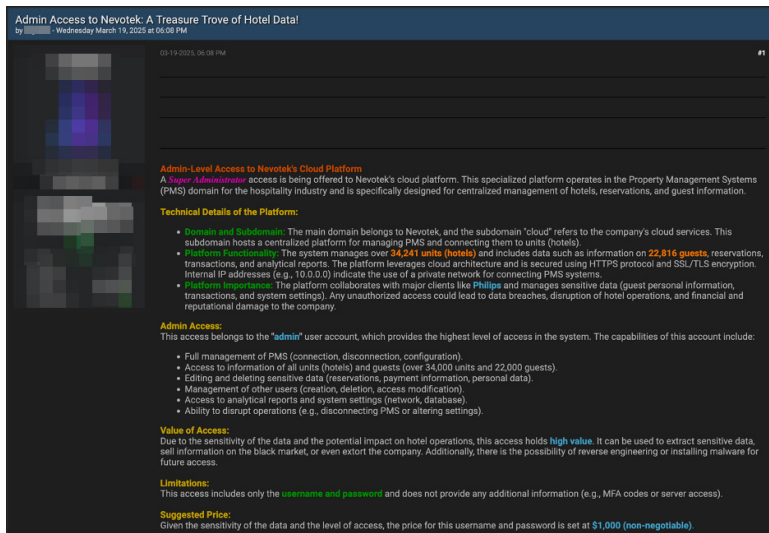


Figure 3. A threat actor offers admin access to a centralized management platform connected to hospitality organizations

In another high-risk scenario, if attackers compromise the admin account of a cloud platform, which integrates with hotel voice, Internet Protocol television (IPTV), and in-room service systems, the fraud opportunities become more

targeted and guest-facing. With administrative control, an attacker could intercept or modify guest communications (e.g., messages or requests sent via in-room tablets), reroute service requests, or inject malicious prompts into the digital concierge systems.

For example, they could send fake upgrade offers or payment links to guests, posing as the hotel, to harvest credit card details. In a more covert approach, they could surveil high-value guests or executive travelers, gathering intelligence from communications and service logs for later social engineering or extortion. Since platforms often operate across multiple hotel branches, a single compromised account can affect several properties at once.

These types of fraud — rooted in deep, persistent access — are particularly dangerous because they don't rely on social engineering or stolen cards alone. Instead, they exploit the trust and automation built into hospitality systems. They allow attackers to operate quietly, systematically, and at scale, making recovery costs significantly higher than from surface-level attacks.

Fraudsters Study and Share Booking Platform Secrets

In underground forums, Telegram groups, and private marketplaces, cybercriminals are actively collaborating, sharing guides, and trading access on how to exploit major booking platforms. These platforms are highly attractive to fraudsters for several reasons: they handle large transaction volumes, operate globally, offer real-time availability, and often serve as intermediaries between guests and property owners with limited direct verification.

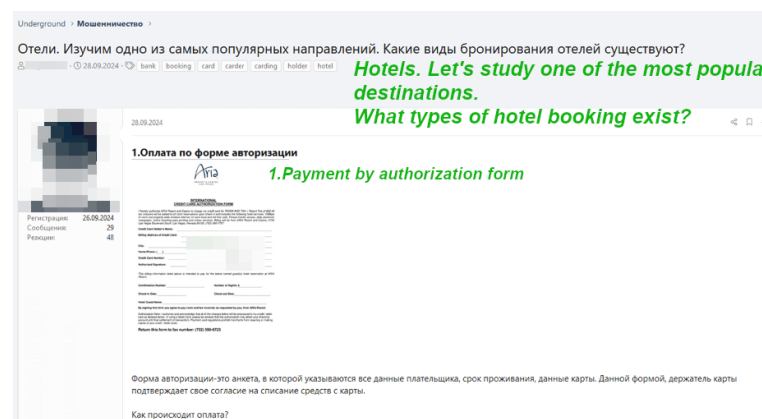


Figure 4. An educational article about hotel booking types on a dark web forum

For criminals, this creates a ripe opportunity to “book now, pay never”, or worse, use the platform as a staging ground for larger financial and logistical fraud schemes.

3.86ив в Booking

Booking.com is one of the largest online apartment booking companies on the market.

How do they work?

The principle of operation is very simple: Hotels post their properties -> Users select suitable ones and pay -> Hotels pay a commission to the site once a month.

Booking does not charge transactions and does not have its own merchant.

When you enter the CC data, Booking sends the entered data to the hotel via a secure channel. The hotel writes off the money at some point in time (at its discretion).

After you have entered it, it is important to monitor the write-off of funds. (By calling the bank, if the transaction is reviewed).

In a situation where the hotel was unable to write off funds from the card, they can write to the email. In this case, you can give another CC.

Then we wait for some time, after which we call the hotel.

We introduce ourselves, inform that we have paid for the room through Booking. We ask you to check whether everything has been paid and whether there are any additional costs.

The downside of this method is that a charge often arrives during your stay. And in such a situation, the person staying has to pay in cash.

Figure 5. Translated booking platform instructions on a dark web forum

Hackers often share detailed tutorials on how to insert stolen credit card data into active bookings, bypass verification checks, and avoid detection. The methods range from using automated card testing scripts to exploiting region-specific policies (like pay-at-property options or delayed payment processing) to socially engineering hotel staff to confirm bookings manually when automated checks fail.

Once a booking is confirmed using stolen or cloned cards, the fraudster may use the reservation for personal travel, resell it on third-party sites, or use the confirmation as proof of legitimacy in another scam, such as visa fraud or money laundering.

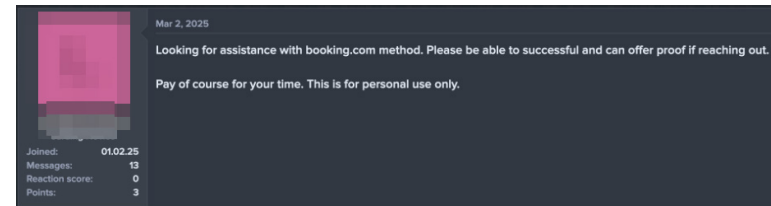


Figure 6. Actor asking for help with booking method, for its own purpose

For hospitality businesses and platforms alike, this trend represents a critical threat. Booking platforms are no longer just service tools — they're targets and enablers of fraud.

Whether fraud takes the form of stolen stays, card abuse, or partner account manipulation, the tactics are evolving fast and being shared in real time among threat actors. Without aggressive fraud detection, closer vetting of partners, and cross-platform intelligence sharing, the hospitality industry remains vulnerable to a coordinated wave of booking abuse.

Cooperative Fraud

One of the more concerning developments in the hospitality threat landscape is the growing presence of cooperation offers on dark web forums, encrypted messaging channels, and invite-only fraud marketplaces. Hospitality fraud is no longer the work of isolated actors; instead, it is increasingly a crowdsourced operation where individuals with different access levels or skill sets are recruited to play a role in complex schemes. This cooperation creates a distributed criminal ecosystem, enabling scalable, sustained attacks on the hospitality sector.

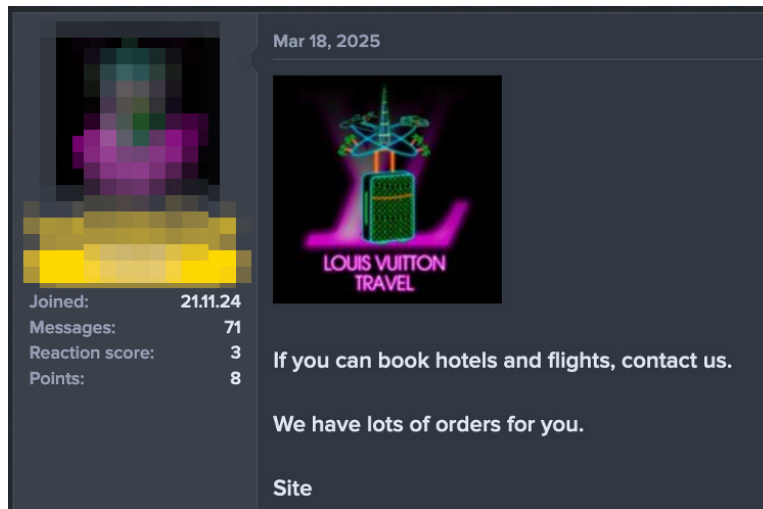


Figure 7. A dark web travel agency is looking for people who could assist in their operations

A common pattern involves actors openly advertising “hotel logs” or admin-level access to hospitality platforms, inviting others to collaborate to generate fraudulent bookings, process fake transactions, or exploit loyalty systems. These sellers often promise a cut of the profits to anyone who can bring buyers, organize travel logistics, or help launder the proceeds. In other cases, buyers are looking to rent or temporarily use hotel access for specific operations, such as inserting stolen card data, modifying back-end reservation records, or using the system as a front to “confirm” fraudulent stays.

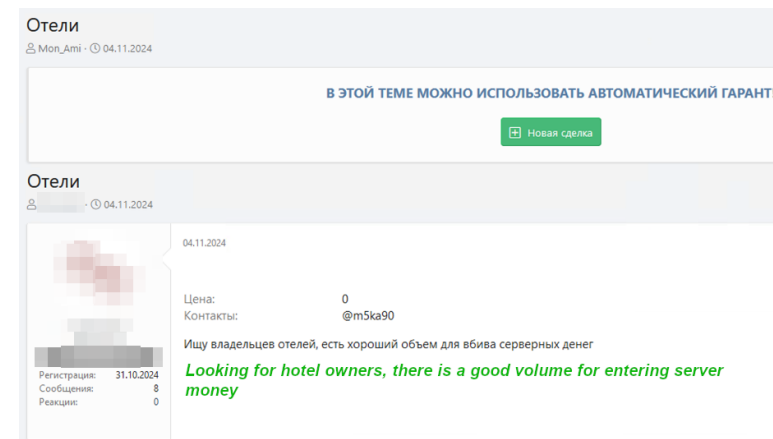


Figure 8. A threat actor is looking for other malicious actors who have access to hotels

Another prominent category involves threat actors actively seeking those who have access to internal systems, such as PMS, POS dashboards, or customer databases. This access is often used for “type in” bookings, override verification steps, or process ghost transactions that align with fraudulent payment flows.

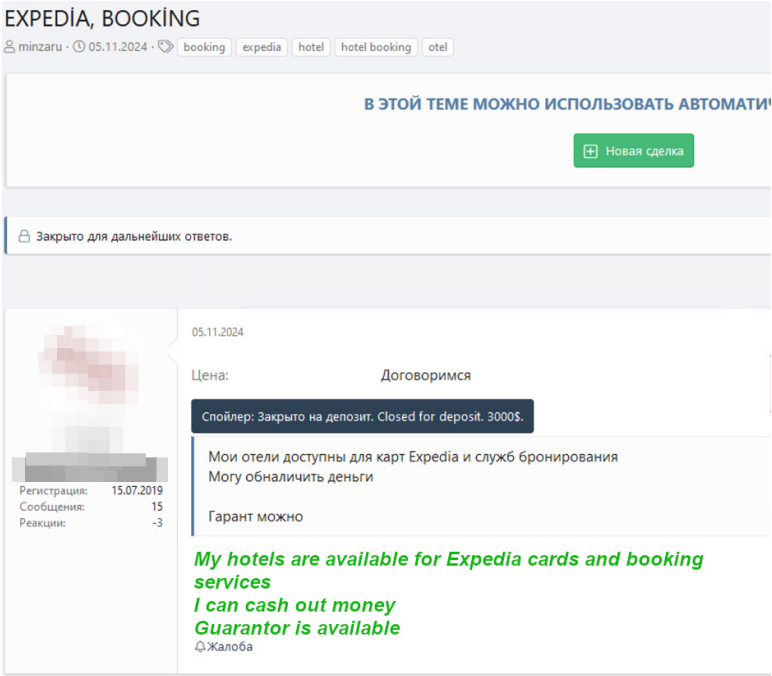


Figure 9. The actor is offering a partnership, making “ready-to-go” hotels available for use

Some actors act as middlemen or coordinators, offering “ready-to-go” hotel listings (often part of a previously compromised franchise or independent property) and looking for partners to supply stolen cards, handle customer communications, or convert loyalty points into bookings. These arrangements often take the form of short-term projects with time-sensitive goals, especially during peak travel periods when fraud is harder to detect.

This collaborative model poses significant risks to the hospitality industry. It multiplies the volume and complexity of fraud attempts, enables persistent insider threats, and lowers the barrier for newcomers to enter the criminal space. For hotels and restaurants, this means fraud can now be injected directly into operational workflows disguised as legitimate internal activity.

Dark Web Travel Agents

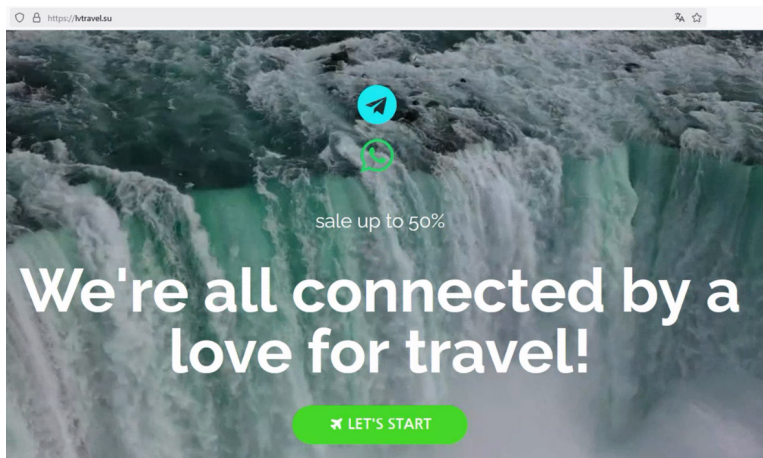


Figure 10. The landing page of a dark web-advertised travel agency

Some malicious operators have been reportedly active on the dark web since 2018, offering heavily discounted “all-in-one” travel packages, claiming savings of 50 to 70% on hotel bookings, international flights, car rentals, and even guided excursions.

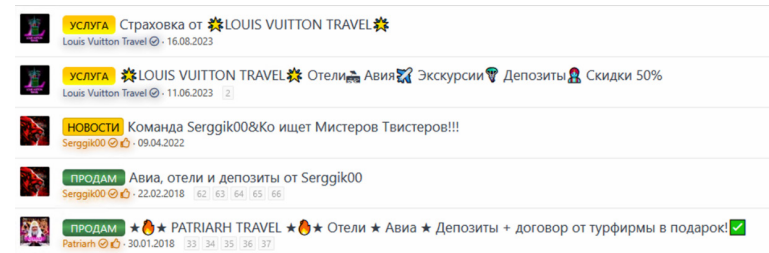


Figure 11. Travel services' offers on a dark web forum, some have been active since 2018

These underground “travel agencies” promise their customers everything from luxury hotel stays and business-class flights to full holiday itineraries at a fraction of the market price. While the pricing may sound too good to be true, the market for such services has grown steadily, with clients ranging from cybercriminals to individuals simply looking for a cheap getaway, knowingly or unknowingly participating in fraudulent activity.

Although these groups do not openly disclose how they operate, their modus operandi likely involves using stolen credit card data, compromised loyalty accounts, or hijacked admin access to travel and booking platforms.

In some cases, hotel reservations or airline tickets may be made using corporate cards, cloned payment data, or laundered cryptocurrency routed through front operations. These services may also exploit vulnerabilities in third-party booking engines or affiliate dashboards, where confirmations can be generated and manipulated before fraud detection tools are triggered.

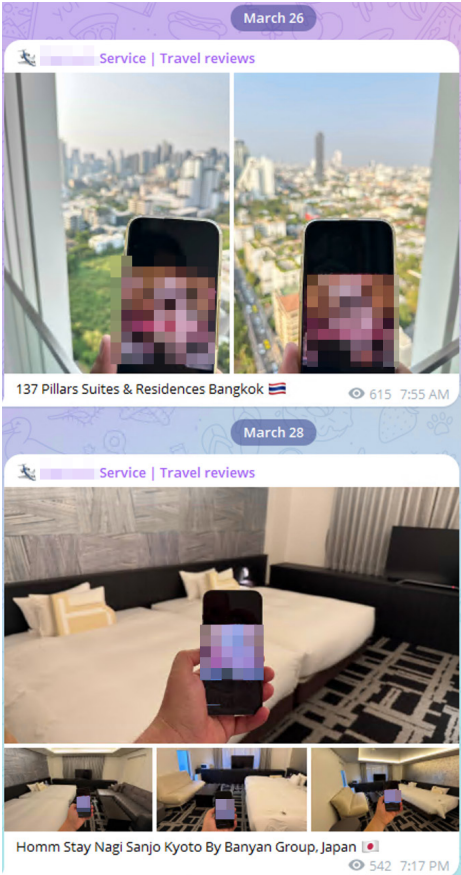


Figure 12. A dark web travel agency shows client reviews that serve as proof of its clients staying in posh on the agency's Telegram channel

One of the striking features of these dark web travel operations is their insistence on tight booking windows, usually three to eight days before travel. This strategy helps reduce the likelihood of detection, cancellation, or chargeback flags before the traveler arrives. Hotels and airlines often do not fully process or verify the validity of a booking until shortly before check-in or boarding, allowing fraudulent reservations to go unnoticed until it's too late to act without disrupting the customer experience.



Figure 13. A dark web travel agency shows a photo of a client that serves as proof of a successful resort stay on the agency's website



Figure 14. A travel agency shares a photo showing a client's booked airline tickets on the agency's Telegram channel

For the hospitality industry, these underground travel schemes present multiple challenges. First, they contribute to chargeback losses and revenue leakage, forcing hotels and airlines to absorb costs tied to fraudulently obtained bookings. Secondly, such fraudulent activity can distort revenue

forecasting, strain staff, and complicate loyalty program analytics. Hotels may also find themselves involuntarily facilitating money laundering, especially when fraudulent bookings are paid using seemingly valid corporate or business-class methods that appear legitimate on the surface.

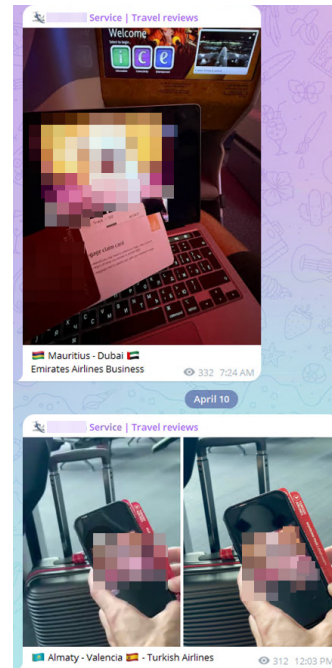


Figure 15. The dark web travel agency's Telegram channel filled with positive feedback from clients

In a broader context, dark web travel agencies reflect how the cybercriminal economy continues to professionalize and diversify. What was once a domain of brute-force hacking and malware is now expanding into full-fledged service ecosystems complete with customer support, referral discounts, and repeat business incentives.

Casino Fraud

Casinos, whether land-based, sea-based or online, represent one of the most lucrative and targeted segments within the hospitality industry. They are high-cash, high-volume environments tightly integrated with hotels, restaurants, VIP services, and financial operations.

As such, casinos are not just places of entertainment, but complex digital ecosystems filled with sensitive personal, financial, and behavioral data. This makes them a magnet for cybercriminals and fraud actors who see in them opportunity and leverage.

Some Casino Fraud Schemes Shared on the Dark Web

Within dark web communities, casino-related fraud is an evolving topic of discussion. Forums feature ongoing conversations among threat actors exchanging ideas. These discussions often blend technical schemes with social engineering and other manipulation tactics.

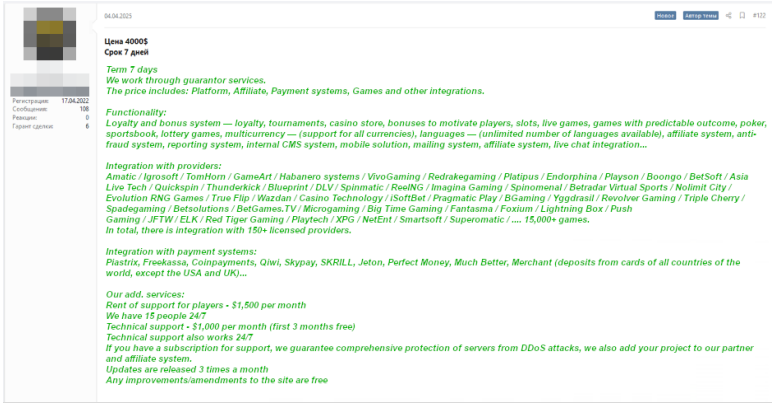


Figure 16. A threat actor promotes website development services including gambling platform integrations

It also appears to go beyond targeting existing casinos and may involve setting up fully fraudulent casinos. One of the most striking observations is the presence of advertisements for B2B-style services, including turnkey integrations with major gambling platforms, payment gateways, and even crypto processors. These service providers claim to assist with launching casino-like projects, complete with game libraries, know your customer (KYC) flows, and full front-end branding. While some of these ads may be connected to gray-market operations, their presence on dark web forums raises an obvious question: Why would a seemingly legitimate service be marketed alongside malware, exploits, and stolen data? Facilitating the creation of fraudulent casinos is one likely answer.

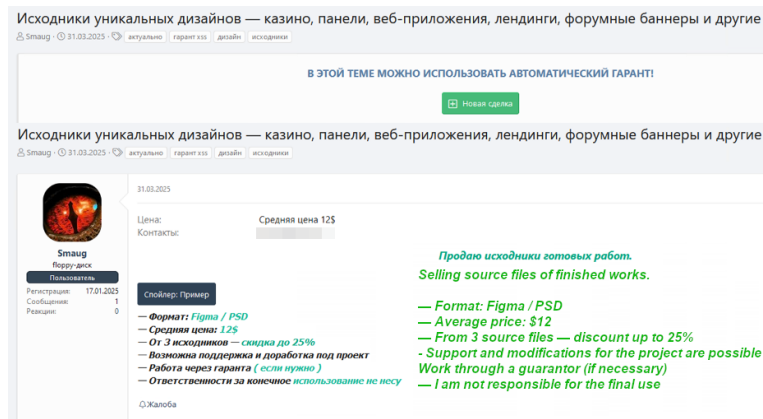


Figure17. A threat actor offers unique casino website designs for sale

In parallel, there is a market for phishing kits specifically tailored to online casinos. Threat actors advertise ready-to-deploy phishing pages that mimic popular gambling brands, including login portals, promotional banners, and fake payment flows.

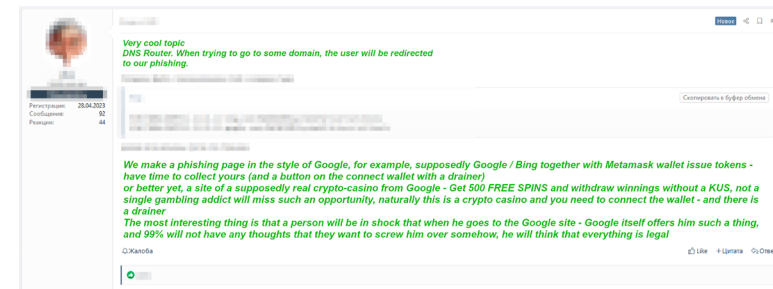


Figure18. A dark web user suggests a method to attract gamblers by redirecting victims to a phishing page with a drainer

Advanced actors may offer custom redirect services — malicious links that initially appear to lead to legitimate redirections but then redirect users to credential harvesting pages or malware loaders. These are often bundled with bulletproof hosting and analytics dashboards to track campaign success.

In addition to targeting users, some discussions pivoted toward questionable or unregulated online casinos themselves. A number of underground operators are believed to run casinos with dual purposes: offering gambling services on the surface while serving as money laundering hubs behind the scenes. This laundering scheme often involves either insiders or colluding users who intentionally “lose” funds during gameplay using illicit proceeds.

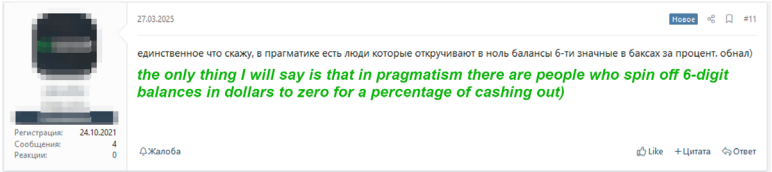


Figure 19. A threat actor on a dark web forum described a money laundering scheme used in a casino

The losing player uses dirty money to fund their bets, while their counterpart (or another account under the control of the launderer) wins and cashes out “clean” money.

This process, often repeated over multiple accounts and sessions, obscures the original source of funds, particularly when payouts are routed through crypto wallets, prepaid cards, or payment services hosted in jurisdictions with lax oversight.

Some of these platforms pose as legitimate operators while others are short-lived or completely fake and are designed purely to cycle money through scripted interactions. These pseudo-casinos accept deposits, simulate activity, and offer payout options with no real gambling occurring at all, just a façade to justify financial flows.

The convergence of fraud-as-a-service, phishing infrastructure, and laundering schemes in the casino space highlights a critical issue for regulators and hospitality-linked platforms. Casinos are, by nature, high-risk and cash-intensive, and they are being weaponized not only as targets of fraud but as tools for facilitating broader financial crime.

Security Recommendations for Hospitality Businesses

Strengthen Access Controls and Credential Security

- Enforce multi-factor authentication (MFA) for all staff-facing systems, including PMS, POS, CMS, and cloud platforms.
- Regularly rotate credentials and audit user roles to prevent unnecessary privilege accumulation.
- Monitor for credential leaks and password reuse through dark web scanning services.

Educate Staff and Monitor for Insider Risk

- Train staff to recognize social engineering, phishing attempts, and signs of internal fraud.
- Implement segregation of duties and monitor high-risk transactions (e.g., refunds, manual overrides).
- Encourage a culture of reporting suspicious behavior without fear of retaliation.

Enhance Technical Defenses

- Use endpoint detection and response (EDR) tools, especially on systems with payment or reservation capabilities.
- Segment networks to separate guest, employee, and critical infrastructure traffic.
- Invest in fraud detection software with behavioral analytics to identify unusual booking patterns or payment behavior.

Audit and Vet Third-Party Vendors

- Conduct thorough security assessments of all booking engines, payment processors, and cloud service providers.
- Include cybersecurity obligations and breach response requirements in vendor contracts.
- Regularly review and monitor integrations with platforms like booking platforms, casino software, or loyalty portals.

Monitor Threat Intelligence and Dark Web Activity

- Stay informed on emerging fraud methods, platform abuse, and underground chatter targeting the hospitality sector.
- Track mentions of your brand, domain, or exposed data in dark web marketplaces.
- Join industry information-sharing groups or ISACs focused on hospitality or retail fraud.

Prepare for Incident Response and Financial Recovery

- Develop and test incident response playbooks tailored to fraud, ransomware, and booking abuse scenarios.
- Establish relationships with law enforcement, payment processors, and cyber insurance providers ahead of time.
- Maintain transaction logs and booking records to support investigations and chargeback defense.

Hospitality is built on trust, service, and experience, but without cybersecurity and fraud prevention at its core, these pillars become fragile. By proactively investing in layered defenses and staying informed on criminal innovation, hospitality businesses can stay one step ahead of fraudsters and continue to deliver the seamless experiences their guests expect and deserve.

