THREAT INTELLIGENCE REPORT

Fake Casino Epidemic: 4 Scam Panels Exposed From the Inside

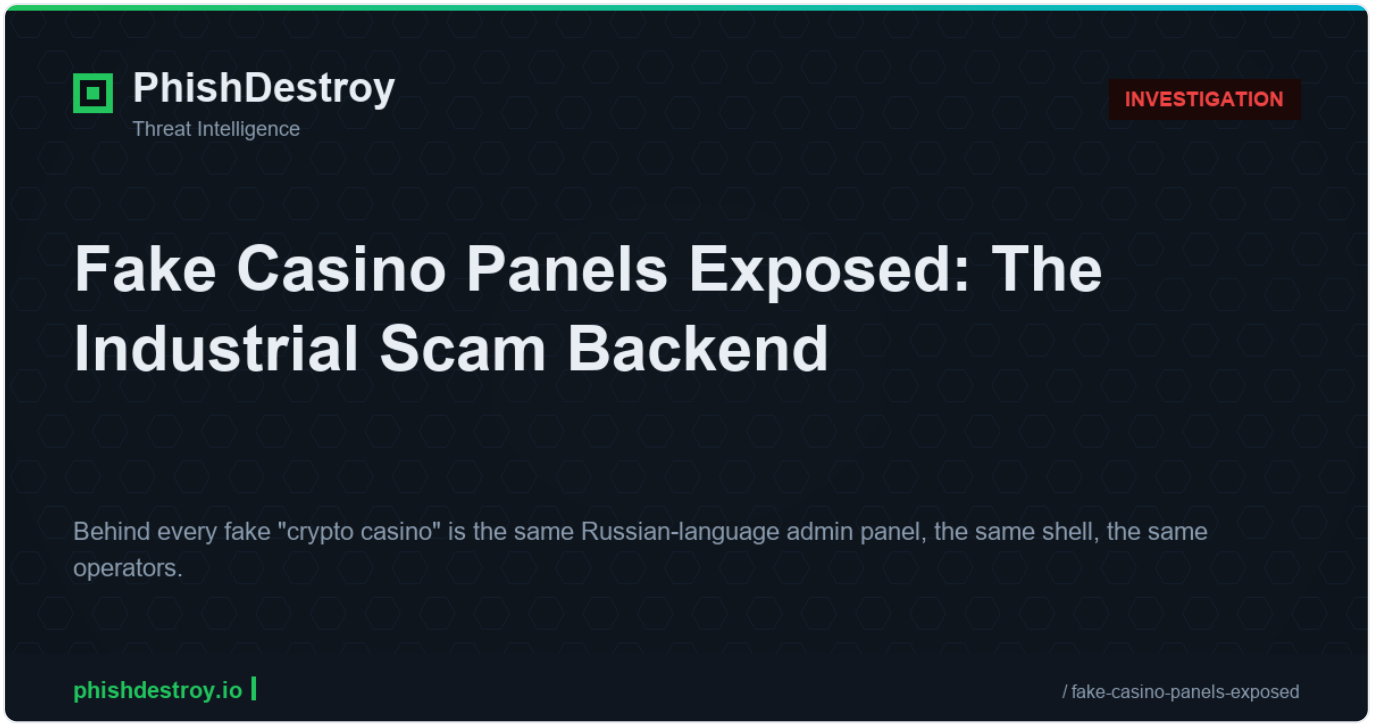
Ref. **PD-TI-2026-72642** Published **10 July 2026** Source **phishdestroy.io/fake-casino-panels-exposed**

ScamIntelLogs Investigation

Comparative anatomy of 4 casino Panel-as-a-Service operations discovered through PhishDestroy's ScamIntelLogs archive. From 383 verified victims across 30+ countries to a meta-scam that steals from its own scammers — every panel, every credential, every lie exposed.

8 min read · Updated **March 2026** · PhishDestroy Intelligence

383 Verified Victims 40+ Phishing Domains 4 Operations Exposed



0
Verified Victims
30+
Countries Targeted
0
Phishing Domains
4
Operations Exposed

The Casino Scam Playbook: How All 4 Panels Operate

Every operation in this investigation follows the same core playbook: build a fake casino or sports betting platform, recruit "workers" (affiliates) through Telegram, lure victims with promises of free bonuses, then trap them with a mandatory "verification deposit" that can never be withdrawn. The victim's money is split between the worker and the panel operator.

What makes this investigation unique is that all four operations were preserved in PhishDestroy's ScamIntelLogs archive — complete with internal Telegram chats, admin panel dumps, configuration files, victim databases, and source code. Every claim below is backed by primary evidence.

Shared DNA

All four panels share: Cloudflare protection, Russian-speaking operators, Telegram-based recruitment, the "verification deposit" scam model, template variables like `%sum_verif%` for deposit amounts, and overlapping domains (**inclusivebets.fun** appears in BOTH OFEDREX and Olympus).

Operation OFEDREX: 383 Victims Across 30+ Countries

OFEDREX, also known as WinSystems and TheProject Casino, is the most documented operation in this investigation. A full admin database dump revealed 383 individual victims across 30+ countries with India leading at 20.1%.

383
Verified Victims
22
Phishing Domains
20.1%
From India
30+
Countries Hit
The operation used promo codes to track affiliate performance. Code **"DREAM"** alone brought in 115 victims. Code **"LRX774"** generated 61 victims.

Leaked credentials found in configuration files:
Email: `lancerbuy777@project.com`
Password: `holabol1337`
Super account keyword: `ximerawork`

— OFEDREX admin configuration dump

Debug Mode Left Enabled

The entire Laravel PHP backend was running with `APP_DEBUG=true` in production, exposing full stack traces, database queries, and internal paths to anyone who triggered an error. This is amateur-hour security that tells you everything about the operators' skill level.

Indicators of Compromise

Domain	Status
winsystems-lp.site	Taken Down
inclusivebets.fun	Active
luckypeak.pro	Taken Down
betmax-official.com	Taken Down

LuxardGambling: Celebrity Deepfakes & "Mammoth" Victims

LuxardGambling operates as a Panel-as-a-Service (PaaS) with 70% commission to workers. What sets it apart is its industrial-scale use of celebrity deepfakes and its brazenly documented playbook published on GitBook.

The operation uses deepfakes of at least 12 celebrities including Elon Musk, MrBeast, Jake Paul, Neymar, and others to create fake endorsement videos. Sports results are inflated by +35% to create the illusion of "guaranteed wins" — a fictional sportsbook called "Crazy Odds" with impossible odds.

"The victim (mammoth) sees inflated coefficients and believes they can predict outcomes. Once they deposit the verification amount, they can never withdraw. The money flows up."

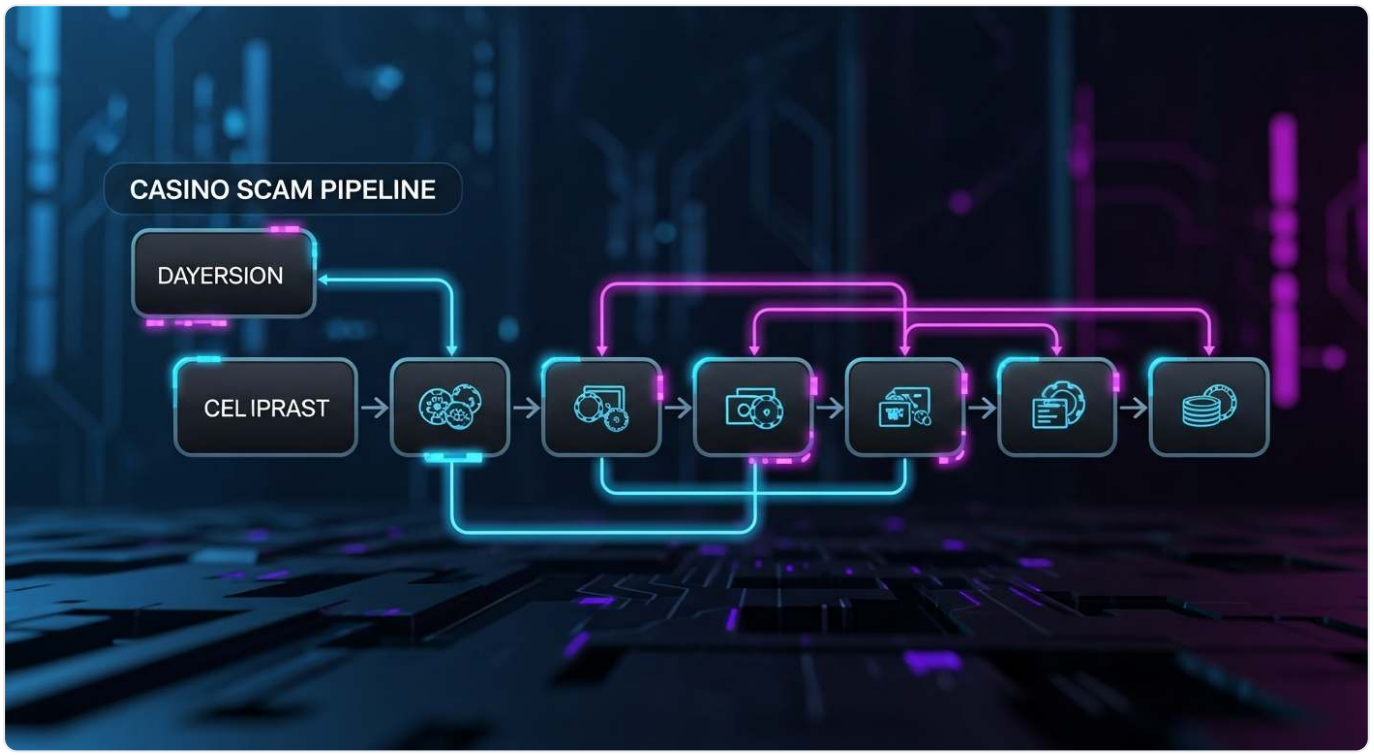
— LuxardGambling GitBook documentation

Deepfake Factory

12+ celebrity deepfakes including Elon Musk, MrBeast, Jake Paul, Neymar, and Travis Scott. Victims are shown fake endorsement videos before being directed to the platform.

Mammoth Hunting

Workers call victims "mammoths" (мамонт). Full trafficking pipeline: fake ad → deepfake video → registration → verification deposit → withdrawal block.



Casino scam pipeline flowchart: from diversion and celebrity endorsement through payment processing to victim

Olympus Panel: The AI Chatbot Trap

Olympus Panel (Syndicate Casino) deployed across 16 domains from a central admin at `olympus-panel.cc` . Its distinguishing feature: "Alice," an AI-powered chatbot deployed on every casino instance to engage victims in real-time conversation and guide them toward the $50 minimum verification deposit.

Workers receive 70% commission. The admin panel HTML dumps show full victim tracking with deposit amounts auto-filled using template variable `%sum_verif%` .

Domain Overlap Detected

The domain **inclusivebets.fun** appears in BOTH the OFEDREX and Olympus databases, suggesting either shared infrastructure, the same operators running multiple panels, or affiliates cross-selling between platforms.

Indicators of Compromise

Domain	Status
olympus-panel.cc	Admin Panel
syndicate-casino.com	Taken Down

Domain	Status
inclusivebets.fun	Shared w/ OFEDREX

BitXLucky: The Scam That Scams Scammers

BitXLucky is the most cynical operation in our archive. Built on Next.js/NestJS, it presents itself as a casino PaaS platform recruiting workers — but registrations from victims never appear in the worker panel. Workers: 0. Every single victim registration is silently redirected to the operator, cutting affiliates out entirely.

This is a **meta-scam** : a scam tool that steals from its own scammers.

Proof Is In The Typos

The admin panel is riddled with spelling errors: "saport" (support), "Warkers" (Workers), "Logi" (Login), "Postsuk" (Postback). These aren't just typos — they're fingerprints of a hastily built fraud tool by non-native speakers.

Worker Dashboard: "Warkers: 0 | Total Deposits: 0 | Logi: saport@bitxlucky"

— BitXLucky admin panel screenshot

Exposed Infrastructure

Server IPs discovered in configuration: `77.110.103.90` `176.46.152.13:3000` `77.221.151.196` . Unlike the other panels, BitXLucky didn't even bother hiding behind Cloudflare consistently — raw server IPs were exposed in API responses.

Evidence & Source Intelligence

OFEDREX Full Database
383 victims, 22 domains, admin configs

LuxardGambling Evidence
Deepfake screenshots, GitBook docs

Olympus Panel Dumps
16 domains, AI chatbot configs

BitXLucky Meta-Scam
Source code, exposed IPs, panel screenshots

#FakeCasino #GamblingScam #CrimePanel #Investigation #OnlineFraud

Related Research

Gambler Panel: Full Network Analysis
Deep dive into the organized crime network operating 1,200+ casino fraud domains.
RublevkaTeam: Russian TON Scam Exposed
Inside the Telegram-native investment scam targeting Russian crypto users.
Crypto Drainer Toolkit Exposed

How TRXDrop and NiceCrypto weaponize wallet connections to steal crypto.

Steam: Not the Good Guy

How Steam’s platform is exploited for phishing and account theft.
