THREAT INTELLIGENCE REPORT

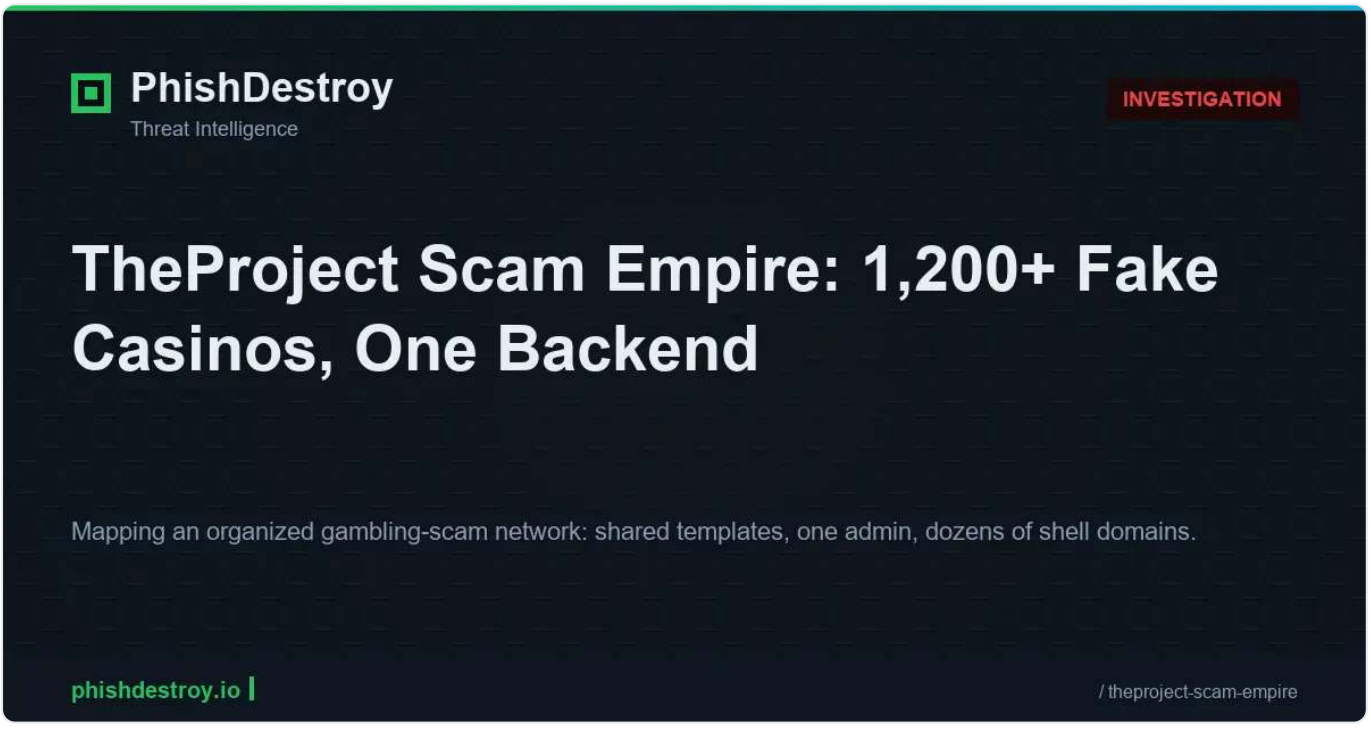
TheProject: Inside a $10M Scam Mentorship Empire Running Since 2021

Ref. **PD-TI-2026-60000** Published **10 July 2026** Source **phishdestroy.io/theproject-scam-empire**

Scam Mentorship Investigation

Not a scam tool — a scam university. TheProject built a hierarchical mentorship machine: recruit, train, deploy, profit. $10M+ claimed revenue, 5,000+ members trained since 2021. Their mentors are the upstream producers behind Gambler, LuxardGambling, and Olympus. They built a school that teaches thousands how to steal.

10 min read · Updated **March 2026** · PhishDestroy Intelligence
$10M+ Claimed Revenue 5,000+ Members Trained 730+ Scammer Usernames Leaked



$10M+
Claimed Revenue
0
Members Trained
0
Scammer Usernames Leaked
0
OFEDREX Victims

The Scam University Model

TheProject is not a tool. It is not a panel. It is not a single scam operation. It is a **school** — a structured, hierarchical mentorship organization that has been training scammers at industrial scale since 2021. Where other investigations expose a product, this one exposes *the factory that produces the producers* .

The operation claims **$10M+ in total revenue** and **5,000+ trained members** . These are not empty boasts. A verified deposit of **₽1M on lolz.live** — the Russian-language cybercrime marketplace — confirms they operate at serious financial scale. Their recruitment thread (`lolz.live/threads/4826265/`) runs openly, advertising mentorship packages to aspiring scammers.

The Hierarchy

Administrators

Top-level operators who control infrastructure, finances, and strategic direction. They manage the platform, set training curricula, and collect the largest share of revenue from all downstream operations.

Mentors

Experienced scammers who train new recruits. Each mentor manages a cohort of workers, provides operational guidance, and takes a percentage cut of every scam their trainees execute. They are the force multiplier.

Workers (Affiliates)

Trained recruits deployed into the field. They run the fake casino sites, manage victim interactions, and process deposits. Revenue flows upward — workers keep a fraction while mentors and admins take the rest.

Victims

End targets across **30+ countries** , with India accounting for **20.1%** of confirmed victims. Victims encounter fake casino platforms, rigged verification deposits, and social-engineered investment traps.

Why This Matters

Most scam investigations focus on a single tool or panel. TheProject is different — it is the **upstream producer** . When you dismantle a Gambler Panel node or shut down a LuxardGambling domain, TheProject simply trains new affiliates and deploys them with fresh infrastructure. You cannot stop the downstream without cutting the supply at the source.

The Casino Pipeline: OFEDREX & WinSystems

TheProject's casino arm operates under the codenames **OFEDREX** and **WinSystems** — a fake casino panel infrastructure that has been directly linked to **383 confirmed victims** across **22 domains** . This is not speculation. PhishDestroy obtained the victim database.

OFEDREX by the Numbers

383 Confirmed Victims

Extracted from leaked databases. Each record includes deposit amounts, geographic origin, and the promo code used to lure them. India leads at 20.1% of total victims, followed by targets across 30+ nations.

22 Active Domains

A rotating fleet of fake casino domains designed to evade takedowns. When one goes down, the infrastructure spawns replacements. All trace back to the same TheProject administrative layer.

Promo Code Tracking

TheProject uses promo codes to track which mentor or affiliate drove each victim. Two codes stand out in the leaked data:

- **DREAM** — 115 victims attributed. Highest-performing affiliate code in the dataset.
- **LRX774** — 61 victims attributed. Linked to a specific mentor cohort operating out of Telegram channels.

SQL Injection Vulnerability

During investigation, PhishDestroy discovered a **SQL injection vulnerability** in TheProject's platform infrastructure. This vulnerability exposed internal database structures and confirmed the authenticity of the leaked victim data. The finding demonstrates that TheProject's own operational security is built on the same cheap, rushed code they teach their affiliates to deploy.

Leaked Credentials

Administrative credentials recovered from the investigation:

`lancerbuy777@project.com / holabol1337`

Super account keyword: `ximerawork`

— Extracted from TheProject infrastructure breach

The Mentorship Hierarchy

TheProject's recruitment pipeline operates in the open. Their primary recruitment thread on **lolz.live** (`threads/4826265/`) advertises mentorship packages with the confidence of a legitimate SaaS business. The ₽1M verified deposit on the platform serves as social proof — a signal to potential recruits that this operation generates real money.

Recruitment Flow

Step 1: Recruitment

New members find TheProject through lolz.live threads, Telegram channels, and word-of-mouth in Russian-language cybercrime forums. The Telegram bot `@TheProject_inbot` (ID: 7291050577) handles initial onboarding and verification.

Step 2: Training

Recruits are assigned to a mentor who teaches them the full scam lifecycle: domain setup, victim acquisition through social engineering, deposit manipulation, and fund extraction. Training materials are structured and standardized.

Step 3: Deployment

Trained affiliates receive access to panel infrastructure (OFEDREX, WinSystems, or external panels like Gambler and Olympus). They launch their own operations under mentor supervision, with revenue sharing enforced through the platform.

Step 4: Profit Extraction

Revenue flows upward through the hierarchy. Workers keep a fraction. Mentors take their cut. Administrators collect from every active operation. The Google Spreadsheet database tracks all financial flows, victim counts, and affiliate performance metrics.

Telegram Bot

`@TheProject_inbot` (ID: 7291050577) — handles onboarding, verification, and basic support for new recruits entering the mentorship pipeline.

Operations Tracking

TheProject uses a **Google Spreadsheet database** to track affiliate performance, victim counts, revenue attribution, and mentor payouts. Centralized, auditable, and damning.

Scale of Operations

With **5,000+ claimed members** and a **₽1M verified lolz.live deposit** , TheProject operates at a scale that dwarfs most individual scam panels. This is organized crime with a corporate structure — recruitment pipelines, training curricula, performance tracking, and revenue sharing agreements.

Downstream Operations: The Training Pipeline

TheProject does not just run scams — it **produces scammers** . PhishDestroy's investigation identified TheProject as the *upstream producer* for multiple well-known scam panel ecosystems. Affiliates trained by TheProject mentors go on to operate:

- **Gambler Panel** — The largest fake casino panel network, with 1,200+ domains tracked by PhishDestroy. TheProject-trained operators represent a significant portion of Gambler's affiliate base.
- **LuxardGambling** — A premium-branded fake casino operation. Shared infrastructure and credential overlaps trace directly back to TheProject's training pipeline.
- **Olympus Panel** — Another downstream panel whose operators were trained through TheProject's mentorship system. Overlapping domain patterns and shared promo codes confirm the connection.

730+ Scammer Usernames Leaked

PhishDestroy's investigation recovered a database of **730+ unique scammer usernames** associated with TheProject operations. This dataset includes Telegram handles, lolz.live accounts, and internal

platform identifiers. It represents one of the largest single leaks of scam affiliate identities ever documented.

The Connection Map

The evidence chain is clear: TheProject trains affiliates. Those affiliates deploy on Gambler, LuxardGambling, and Olympus panels. Shared credentials (`lancerbuy777@project.com`), overlapping domains, and leaked databases prove these operations are not independent — they are **downstream products of TheProject's training pipeline** . Shut down a Gambler node and TheProject deploys ten more graduates.

"They built a school that teaches thousands how to steal."

— PhishDestroy Research Assessment

Evidence & Source Intelligence

All findings in this investigation are backed by primary source evidence preserved in PhishDestroy's ScamIntelLogs repository. The following indicators of compromise (IOCs) and evidence artifacts are publicly available for verification.

Key IOC Table

Indicator	Type	Value
Telegram Bot	Bot ID	@TheProject_inbot (7291050577)
Forum Thread	URL	lolz.live/threads/4826265/
Leaked Credential	Email/Password	lancerbuy777@project.com / holabol1337
Super Account	Keyword	ximerawork
Promo Code (Top)	Tracking Code	DREAM (115 victims)
Promo Code	Tracking Code	LRX774 (61 victims)
Casino Component	Panel Name	OFEDREX / WinSystems
OFEDREX Victims	Count	383 confirmed
OFEDREX Domains	Count	22 active domains

Evidence Repository

ScamIntelLogs: TheProject

Full evidence archive including leaked databases, affiliate lists, domain records, and infrastructure mapping.

ScamIntelLogs Repository

PhishDestroy's public intelligence repository — all investigations, IOCs, and evidence preservation.

Live Threat Map

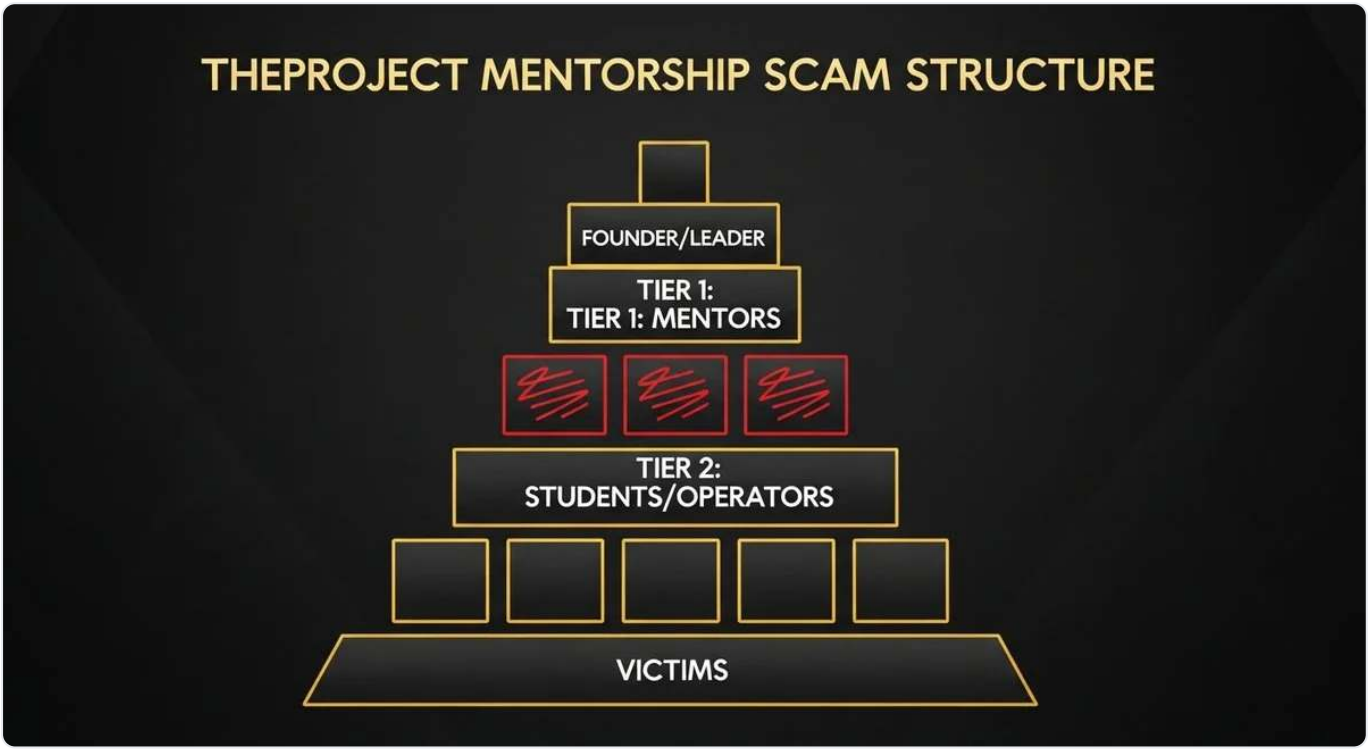
Real-time tracking of active drainers, fake casinos, and phishing nodes linked to TheProject infrastructure.

Report Threats

Encountered a TheProject-linked domain? Report it directly to PhishDestroy for investigation and takedown.

#TheProject #ScamMentorship #CryptoFraud #Investigation #MLM

Related Research



The Project scam empire — pyramid hierarchy and operator roles

Gambler Panel: Full Network Analysis
Deep dive into organized crime infrastructure operating 1,200+ fraudulent casino domains downstream of TheProject.

Fake Casino Epidemic: 5 Panels Exposed
Investigation exposing OFEDREX, LuxardGambling, Olympus Panel, and BitXLucky with leaked credentials and victim databases.

Crypto Drainer Toolkit Exposed
Technical analysis of crypto drainer infrastructure used by TheProject-trained affiliates to steal digital assets.