THREAT INTELLIGENCE REPORT

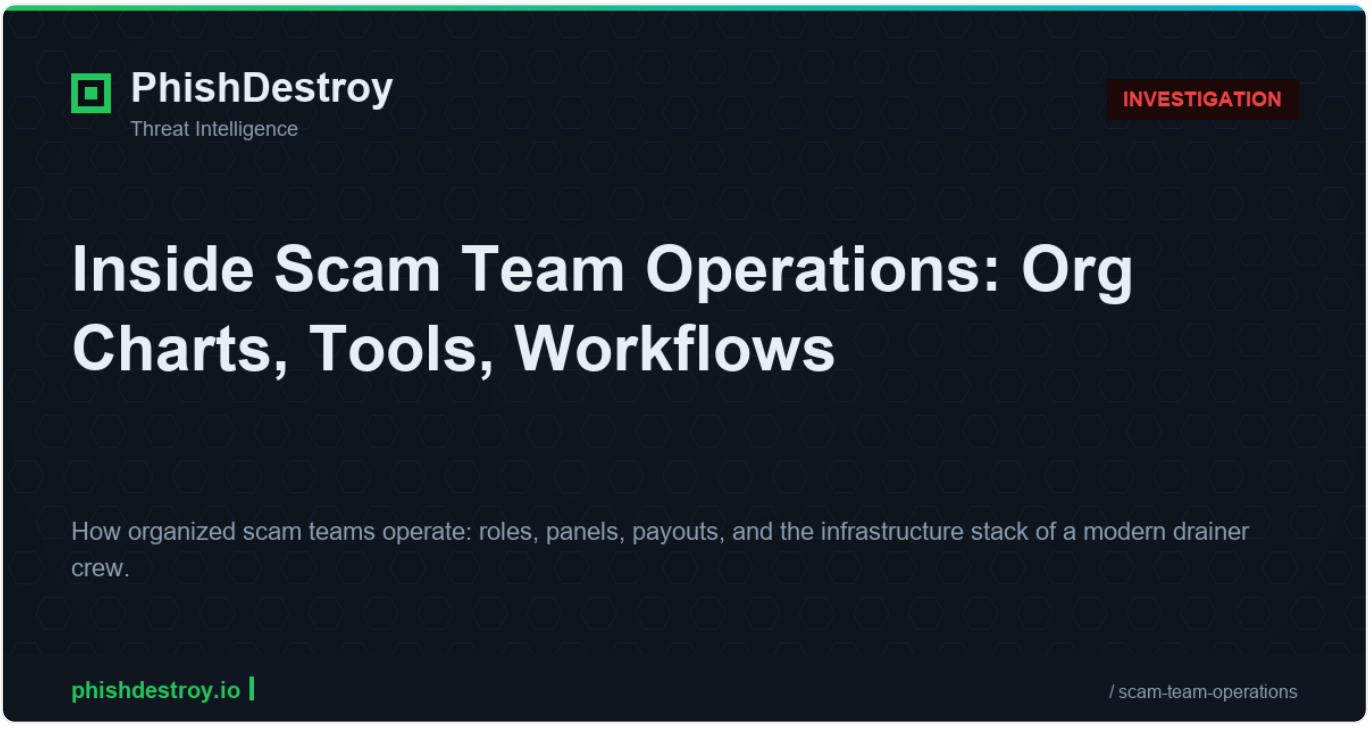
Scam Teams Compared: MercuryTeam, WasabiSquad, and 717Team Operations

Ref. **PD-TI-2026-97291** Published **10 July 2026** Source **phishdestroy.io/scam-team-operations**

~12 min read | investigation

For every billion-dollar headline, there are hundreds of teams like these. Three case studies into the "middle class" of fraud — how mid-tier scam teams recruit, operate, and get disrupted. MercuryTeam runs dual-bot exchange and casino fraud. WasabiSquad deploys a triple threat. 717Team was archived — proof that OSINT disruption works.

11 min read · Updated **March 2026** · PhishDestroy Intelligence
3 Teams Investigated Shared Google Spreadsheet 1 Team Disrupted



3
Teams Investigated
0
717Team Members Tracked
0
Wallets Identified
$2,946
Confirmed Drained (717Team)

The Middle Class of Fraud

When crypto scam investigations make headlines, the numbers are staggering — $10 million mentorship empires, billion-dollar rug pulls, state-sponsored laundering networks. But beneath those headline-grabbing operations lies a vast ecosystem of **mid-tier scam teams** that collectively cause enormous damage while flying under the radar.

These are not lone actors. They are organized, they recruit through forums, they use Telegram bots for automation, and they track their victims in Google Spreadsheets like any legitimate sales team tracks leads. They represent the **operational middle class of cybercrime** — sophisticated enough to scale, small enough to evade attention.

This investigation examines three such teams documented in PhishDestroy's ScamIntelLogs repository:

MercuryTeam

Status: Active. Dual-vector operation running exchange fraud and casino scams simultaneously through two Telegram bots. Russian-speaking, mentor-based structure.

WasabiSquad

Status: Active. Triple-threat operation targeting victims through fake exchanges, gambling platforms, and investment bots. Shares infrastructure with MercuryTeam.

717Team

Status: ARCHIVED. 125-member operation shut down through intelligence gathering and coordinated reporting. Proof that disruption works.

Key Finding

MercuryTeam and WasabiSquad share the SAME Google Spreadsheet URL — evidence of either identical operators or a tightly coordinated alliance.

Why Mid-Tier Teams Matter

For every billion-dollar headline, there are **hundreds of teams like these** operating daily. They recruit aggressively, iterate rapidly, and collectively drain millions from victims worldwide. Understanding their structure is essential to disrupting them at scale.

MercuryTeam: Dual-Vector Operations

MercuryTeam operates a **dual-vector fraud model** — running exchange scams and casino scams simultaneously through two dedicated Telegram bots. This approach maximizes victim coverage: users who wouldn't fall for a fake exchange might be lured by a casino offer, and vice versa.

Telegram Bot Infrastructure

Bot	Telegram Handle	Bot ID	Vector
Primary Bot	@MercuryTeam_bot	6631580796	Exchange Fraud

Bot	Telegram Handle	Bot ID	Vector
Casino Bot	@MercuryCasi_bot	6431207710	Casino Fraud

The dual-bot architecture is not accidental. By separating exchange and casino operations into distinct bots, MercuryTeam achieves **operational compartmentalization** — if one bot gets reported or banned, the other continues functioning. Victims interact with whichever bot matches their vulnerability profile.

Organizational Structure

MercuryTeam employs a **mentor model with branches** . Senior operators train recruits who then establish semi-independent branches. This franchise-like structure allows the team to scale rapidly while maintaining operational security. New recruits learn victim engagement techniques, script handling, and withdrawal procedures from their assigned mentors before operating solo.

Forum Presence

MercuryTeam recruits and advertises through **lolz.live** , one of the largest Russian-language fraud forums. Their recruitment thread: `lolz.live/threads/6129774/`

Victim Tracking

Revenue and victim data are tracked through a **shared Google Spreadsheet** — a detail that becomes critical when examining WasabiSquad's operations.

Intelligence Assessment

MercuryTeam represents an **evolution in mid-tier fraud** : the dual-vector approach doubles their attack surface while the mentor model ensures consistent quality across branches. Russian-speaking operation with all coordination conducted through Telegram. Full evidence preserved in ScamIntelLogs.

WasabiSquad: Triple Threat

Where MercuryTeam runs two vectors, WasabiSquad pushes it to **three** — combining fake exchanges, gambling platforms, and investment bots into a single operation. This multi-vector approach targets completely different victim psychologies: the crypto trader, the gambler, and the passive investor.

Bot & Web Infrastructure

Asset	Identifier	Type
Primary Bot	@WasabiSquad_Bot	Telegram Bot (ID: 7380099926)
Website	wasabihub.one	Web Platform
Forum Thread	lolz.live/threads/7933252/	Recruitment & Advertising

Three Attack Vectors

Exchange Fraud

Fake cryptocurrency exchange platforms designed to steal deposits. Victims believe they are trading on a legitimate platform and deposit funds that cannot be withdrawn.

Gambling Fraud

Rigged gambling platforms that promise winnings but require "verification deposits" before withdrawals — deposits that are immediately drained.

Investment Bot Fraud

Automated investment bots that promise guaranteed returns. Victims deposit crypto expecting algorithmic trading profits and receive nothing.

The Spreadsheet Link

WasabiSquad uses the SAME Google Spreadsheet as MercuryTeam for tracking victims and revenue. This is the single most important finding of this investigation.

"Same spreadsheet. Same tracking columns. Same revenue formulas. Either these are the same people wearing different masks, or they trust each other enough to share their entire victim database."

— PhishDestroy Intelligence Assessment

Critical Infrastructure Overlap

The shared Google Spreadsheet between MercuryTeam and WasabiSquad is not a minor technical detail — it is **evidence of operational unity** . Two teams with distinct brands, different Telegram bots, and separate forum threads are using the same backend document to track victims and revenue. This points to either **the same operators running both brands** or a **formal alliance with shared financial infrastructure** .

717Team: Proof Disruption Works

Of the three teams examined in this investigation, 717Team holds a unique distinction: **it has been archived** . In ScamIntelLogs terminology, "archived" means operations have been disrupted and the team is no longer actively scamming. This is not a theoretical success — it is documented proof that intelligence gathering, evidence preservation, and coordinated reporting can shut down organized fraud.

717Team by the Numbers

0
Members Tracked
0
Wallets Identified
$2,946
Confirmed Drained
ARCHIVED
Operations Status

Admin & Network Links

Role	Identifier	Details
Admin	@imdebank	Telegram ID: 7149807602
Network Link	RublevkaTeam	Admin @imdebank linked to this separate operation
Bot	@team717_bot	Primary Telegram bot (now inactive)
Forum	lolz.live	Recruitment and coordination hub

Domain Infrastructure (12+ domains)

Domain	Purpose
checkscore.cc	Primary scam platform
cryptomus-payment.com	Fake payment gateway
check-score.ru	Russian-targeting variant
+ 9 additional domains documented in ScamIntelLogs	

Why Archived Matters

717Team's archived status is the **most important data point** in this entire investigation. It demonstrates that mid-tier scam teams *can* be disrupted through systematic intelligence gathering. The process that worked: (1) identify infrastructure, (2) track wallets and members, (3) preserve evidence, (4) coordinate reporting across platforms. The $2,946.25 confirmed drained represents documented losses — the real figure was likely higher, but the operation was stopped before it could scale further.

The RublevkaTeam Connection

Admin @imdebank (ID: 7149807602) was linked to **RublevkaTeam** , a separate scam operation documented in our Russian TON Scam investigation. This cross-team connection reinforces a central finding: these operations are not isolated. Operators move between teams, share infrastructure, and maintain networks that survive individual team disruptions.

The Shared Infrastructure

Examining these three teams side by side reveals something far more significant than individual operations — it reveals a **network** . Shared tools, shared platforms, shared documents, and in at least one case, a direct personnel link between teams.

Comparative Analysis

Attribute	MercuryTeam	WasabiSquad	717Team
Attack Vectors	Exchange + Casino	Exchange + Gambling + Investment	Exchange + Fake Payments
Forum	lolz.live	lolz.live	lolz.live
Telegram Bots	2 bots	1 bot + website	1 bot
Tracking	Google Spreadsheet	SAME Spreadsheet	Internal tracking
Language	Russian	Russian	Russian

Attribute	MercuryTeam	WasabiSquad	717Team
Status	Active	Active	Archived

Common Infrastructure Points

- **Shared Google Spreadsheet** — MercuryTeam and WasabiSquad use the same document for victim/revenue tracking
- **lolz.live as Central Hub** — All three teams recruit, advertise, and coordinate through the same Russian-language forum
- **Telegram as Operations Layer** — Every team relies on Telegram bots for victim onboarding and operator communication
- **Cross-Team Personnel** — 717Team admin @imdebank linked to RublevkaTeam, demonstrating operator mobility between teams
- **Russian-Language Operations** — All teams operate in Russian, indicating a common geographic and cultural origin

"They share spreadsheets. They share forums. They share techniques. The only thing they don't share is their brand name — and even that distinction might be artificial."

— PhishDestroy Analysis Summary

Not Isolated Actors

The evidence is clear: MercuryTeam, WasabiSquad, and 717Team are not independent operations that coincidentally use similar methods. The **shared Google Spreadsheet** between Mercury and Wasabi, the **shared forum** across all three, and the **personnel overlap** between 717Team and RublevkaTeam all point to an interconnected ecosystem. Disrupting one team without understanding the network risks simply displacing operators to another brand.

Evidence & Documentation

All intelligence referenced in this investigation has been preserved in PhishDestroy's ScamIntelLogs repository. Each team has a dedicated evidence directory containing bot IDs, wallet addresses, forum screenshots, domain lists, and structural analysis.

MercuryTeam Evidence

Dual-bot IDs, forum thread, mentor structure documentation, spreadsheet reference

WasabiSquad Evidence

Triple-threat analysis, wasabihub.one documentation, shared spreadsheet proof

717Team Evidence (Archived)

125 members, 85 wallets, $2,946.25 drained, 12+ domains, admin @imdebank linked to RublevkaTeam

Full ScamIntelLogs Repository

Complete threat intelligence archive — all teams, all evidence, version-controlled

#ScamTeams #MercuryTeam #WasabiSquad #717Team #Investigation

Related Research

TheProject: $10M Scam Mentorship Empire
How a single operation built a $10M mentorship empire teaching others to scam at scale.
Fake Casino Epidemic: 5 Panels Exposed
Inside the fake casino scam panels — OFEDREX, LuxardGambling, Olympus Panel, and BitXLucky exposed.
RublevkaTeam: Russian TON Scam Exposed
Deep dive into RublevkaTeam's TON blockchain scam — linked to 717Team admin @imdebank.