

Operation Scam Hunter

Exposing an 8-Month International Financial Fraud Network



OBJECTIVE OF THE INVESTIGATION

The purpose of this investigation is to identify, document, and consolidate technical evidence related to an international online fraud operation. This report collects and organizes information that enables the relevant authorities — including law enforcement, financial regulators, domain registrars, hosting providers, and browser security teams — to act quickly and take down the infrastructure used by the scammers.

SKILLS DEMONSTRATED

- OSINT & Reconnaissance (WhoIS, DNS analysis, reverse IP lookup)
- Web Application Security (Authentication testing, vulnerability assessment)
- Network Analysis (Port scanning, service enumeration, infrastructure mapping)
- Threat Intelligence (Pattern recognition, timeline analysis, TTP documentation)
- Digital Forensics (Evidence collection, data correlation, chain of custody)
- Ethical Hacking (Boundary awareness, responsible testing)
- Incident Analysis (Root cause investigation, impact assessment)

Fábio Vieira
November 2025

Operation Scam Hunter: Exposing an 8-Month International Financial Fraud Network..	1
INITIAL DISCOVERY & CONTEXT	4
HOW IT REACHED ME:.....	4
INITIAL EVIDENCE:.....	4
KNOWN SCAM INDICATORS:.....	4
INITIAL DOMAIN/ INFRASTRUCTURE ANALYSIS	4
Connected Network Discovery	5
Probable Administrative Functions	8
Infrastructure Role:	8
Protection Level: MEDIUM-HIGH	8
INITIAL VICTIM RESEARCH	9
SCAM METHODOLOGY DOCUMENTATION (FROM VICTIMS).....	10
LEGITIMACY CHECKS PERFORMED	11
TECHNICAL SECURITY ASSESSMENT	12
HTML Source Code Analysis	12
Brand Impersonation	12
Fake Wallet/Payment System	12
Fake Financial Products	12
Fake Real-Time Data	13
Suspicious Service Worker	14
No Regulatory Compliance.....	14
User Account Control	14
AUTHENTICATION SYSTEM TESTING.....	14
Phase 1: SQL Injection Attempts	15
Phase 2: Hydra Brute Force Attack	15
Admin Account Compromise & Operator "ddos" Role Analysis.....	15
Compromised Account Context:	16
Fake Administrative Hierarchy	16
Technical Evidence of Obscured Infrastructure:	16
Script Architecture Analysis:.....	17
Directory Structure Revelations:.....	17
Path Disclosure Evidence:.....	17

Template System Failures:	17
Asset Isolation:	17
THE DOCUMENT UPLOAD TRAP FOR WITHDRAWALS.....	17
The Mechanism.....	18
Possible Malicious Objectives	18
CONCLUSION & RESPONSIBLE DISCLOSURE.....	18
Executive Summary of a Sophisticated Fraud Network.....	19
Key Findings of the Network	19
Immediate Action: Handover to Authorities and Platforms.....	19

INITIAL DISCOVERY & CONTEXT

HOW IT REACHED ME:

I received a message talking about a new method of making money where you could earn money with simple tasks like liking posts, and that it then evolved into a foolproof method linked to cryptocurrency trading, always earning 30%, you just had to join the Telegram group. Unfortunately, I didn't have access to the group, but I got curious and did some research.

<https://www.wct.autos/Trade/index>



INITIAL EVIDENCE:

- Communication: Telegram messages promising easy money for tasks
- Method: "Complete simple tasks → Get paid → Upgrade to higher rewards"
- Platform: Reference to a professional-looking website (wct.autos)
- Red Flags: Guaranteed 30% returns, pressure to recruit others, requests for deposits

KNOWN SCAM INDICATORS:

- Unrealistic profit promises (consistent 30% returns)
- Pyramid-style recruitment requirements
- Pressure to make increasingly larger deposits
- Professional-looking but unverifiable platform
- Use of popular exchange names (Bitfinex) without authorization

INITIAL DOMAIN/ INFRASTRUCTURE ANALYSIS

Starting Point: **wct.autos**

```
(joe@vbox)-[~]
$ nslookup www.wct.autos
Server: 192.168.1.254
Address: 192.168.1.254#53

Non-authoritative answer:
Name: www.wct.autos
Address: 38.181.53.143

(joe@vbox)-[~]
$ whois 38.181.53.143
```

Findings:

Registration: **Belize** (offshore jurisdiction)

Registrar: **Dynadot LLC**

Creation Date: October 10, 2025

Name Servers: NS1.DYNA-NS.NET, NS2.DYNA-NS.NET

Privacy Protection: Enabled (red flag for financial platform)

Location: **Hong Kong**

ISP: HONG KONG COMMUNICATIONS INTERNATIONAL CO., LIMITED

Network: Cogent Communications (US company, Hong Kong routing)



Belize registration + Hong Kong hosting = classic scam infrastructure pattern. Offshore jurisdictions combined with Asia-based hosting provide maximum anonymity for operators.

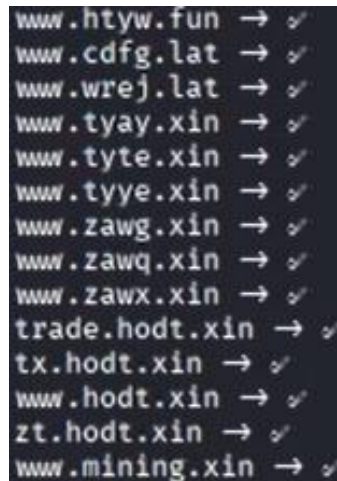
Connected Network Discovery

I discovered this wasn't an isolated operation but part of a larger network:

```
curl -s "https://api.hackertarget.com/reverseiplookup/?q=38.181.53.143"
```

Connected Domains Identified:

www.htyw.fun
www.cdfg.lat
www.wrej.lat
www.tyay.xin
www.tyte.xin
www.tyye.xin
www.zawg.xin
www.zawq.xin
www.zawx.xin
trade.hodt.xin
tx.hodt.xin
www.hodt.xin
zt.hodt.xin
www.mining.xin



```
www.htyw.fun → ✓  
www.cdfg.lat → ✓  
www.wrej.lat → ✓  
www.tyay.xin → ✓  
www.tyte.xin → ✓  
www.tyye.xin → ✓  
www.zawg.xin → ✓  
www.zawq.xin → ✓  
www.zawx.xin → ✓  
trade.hodt.xin → ✓  
tx.hodt.xin → ✓  
www.hodt.xin → ✓  
zt.hodt.xin → ✓  
www.mining.xin → ✓
```

Identified Patterns:

.xin domains (China)

.lat domains (Latin America)

.fun domains (International)

Multiple subdomains (trade., tx., zt.)

Most of them no longer exist/work; some even led me to the Firefox protection page. I know that at the moment **wct** and **cdfg** are the only ones open, but this showed a systematic system of:

- Temporary domains lasting months.
- Constant infrastructures, same IP, same code .
- Different names but the same operation.

Browsing Scan

During the browsing reconnaissance on the target wct.autos, multiple directory paths were discovered. However, most attempts resulted in error responses, only the /admin endpoint was accessible.

Professional admin portal paired with poorly made scam site - this is classic fraud infrastructure.



This probably represents the operational nerve center of the entire scam operation - a professionally crafted Chinese-language administrative panel discovered through systematic error analysis and infrastructure mapping.

"网站管理中心" (Website Management Center)

"用户名" (Username)

"密码" (Password)

"图形验证码" (Graphical Verification Code)

"登录" (Login)

Probable Administrative Functions

Based on the professional implementation, this panel likely controls:

- Victim Management
- View all registered users and their "balances"
- Monitor deposit/withdrawal attempts
- Manage communication logs

System Configuration

- Domain and branding settings
- Security parameter adjustments
- Template and content management

Analytics & Monitoring

- Victim behavior tracking
- Performance metrics
- Security event logging
- Strategic Importance
- Central Command Structure

Infrastructure Role:

hodt.xin (Backend Core)

↓

Manages Multiple Scam Frontends

↓

cdfg.lat → wct.autos → [Additional Domains]

↓

Telegram @Bitfinex0088 (Victim Communication)

Protection Level: MEDIUM-HIGH

Effective Security Measures:

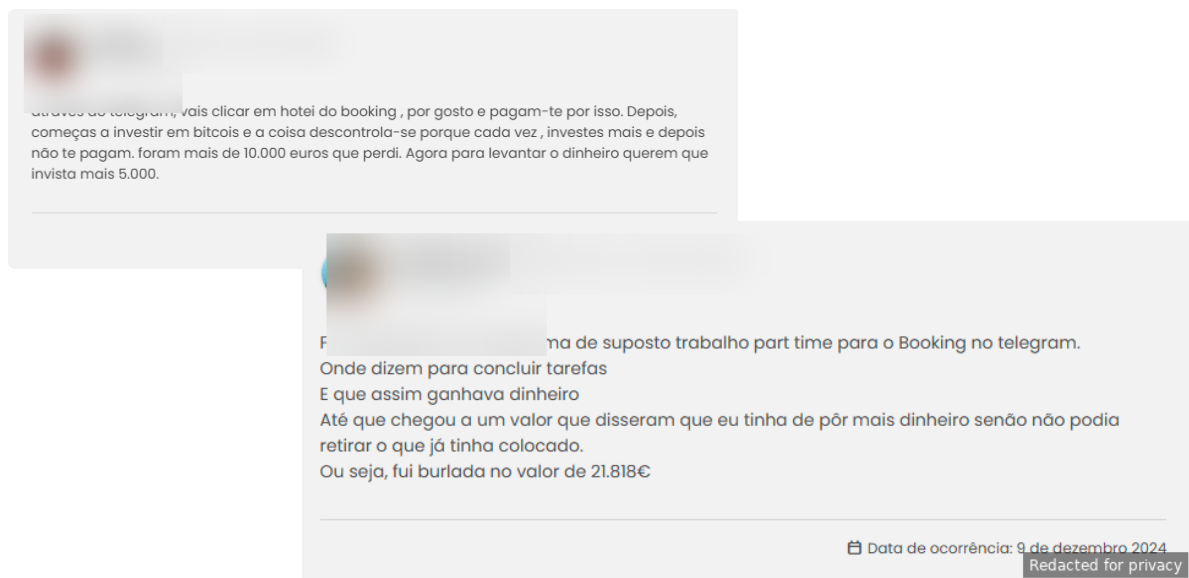
- CAPTCHA implementation prevents automated attacks
- Input sanitization blocks SQL injection
- Session-based authentication
- Professional error handling (in production areas)

VICTIM RESEARCH

Technical analysis alone isn't enough - real victim reports provide the social proof needed to justify further investigation.

On the website "Portal da queixa" that functions as a public complaints site, I found the following statements.

<https://portaldaqueixa.com/brands/bitfinex/complaints/bitfinex-burla-137892625>

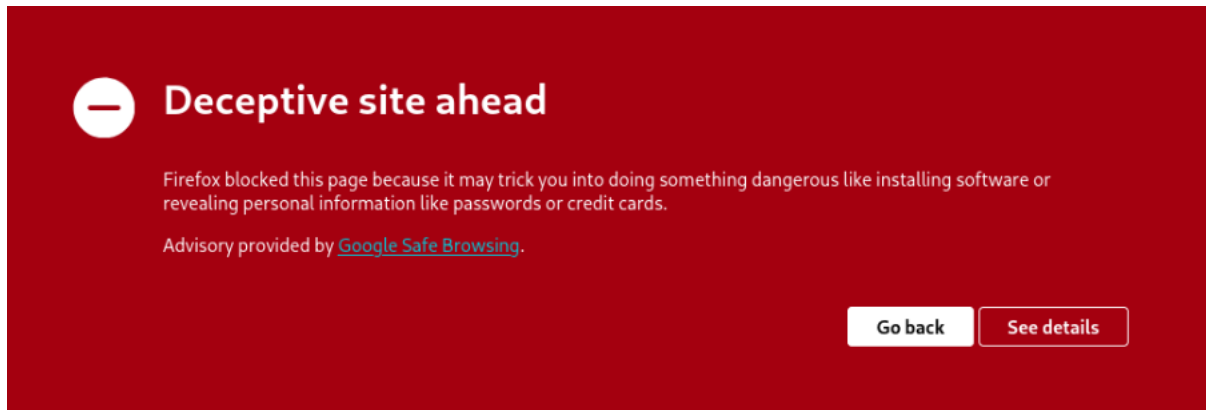


Translation:

Image 1 - "Through Telegram, you click on a hotel on Booking.com, leave a like, and they pay you for it. Then, you start investing in Bitcoin and things get out of control because you invest more and more, and then they don't pay you. I lost over €10,000. Now, to withdraw the money, they want me to invest another €5,000."

Image 2 - "I was lured into a supposed part-time job scheme for Booking on Telegram. They said to complete tasks
And that's how I earned money
Until it reached a certain amount where they said I had to put in more money or I couldn't withdraw what I had already put in.
In other words, I was scammed out of €21,818."

Then I continued searching for victims on social media, where I found several reports from Angola of a Bitfinex with exactly the same interface and method as those we've seen so far, but with two new domains, fekcmdn.vip and asdfeqow.vip. I know they were active in March; both led us here.



These two didn't lead me anywhere; besides being registered in Dubai, they were also much more thoroughly deleted than the others. I found little to nothing about these domains. Here are the websites/methods I used:

- `dig any/mx/txt`
- DNSDUMPSTER
- CRT.SH
- URLSCAN.IO
- ARCHIVE.ORG / CACHE
- WHOIS

From what little I've found, it seems this is probably another scammer network using the exact same method/interface.

SCAM METHODOLOGY DOCUMENTATION (FROM VICTIMS)

Compiled from victim reports:

SCAM PATTERN IDENTIFIED

1. Initial Contact: Telegram/WhatsApp 'job offers'
2. Trust Building: Small real payments (€5-€20)
3. Escalation: 'Upgrade' requests with deposit requirements
4. Extraction: MBWay transfers to provided numbers
5. Disappearance: Account blocking after substantial deposits

Specific numbers identified from victim reports:

966XXXXXX (NOS)

914XXXXXX (Vodafone)

LEGITIMACY CHECKS PERFORMED

LEGITIMACY CHECKS:

- Company Registration: No legitimate business registration found.
- Financial Licensing: No BaFin, SEC, or CMVM authorization.
- Legal Address: Virtual office in Belize, no physical presence.
- Contact Information: Only Telegram/WhatsApp, no verifiable contacts.
- User Reviews: Only victim complaints, no legitimate users.

They claim to have and show a certificate, which is obviously fake since companies/websites registered in Belize, as is obvious, do not have American jurisdiction.



System could not find matching data.

How do I search for MSB
Registration Information?



MSB Registration Status Information

Date: 05/12/2022

The inclusion of a business on the MSB Registrant Search Web page is not a recommendation, certification of legitimacy, or endorsement of the business by any government agency.

The MSB Registrant Search Web page, which is updated on a weekly basis, contains entities that have submitted to Money Services Business (MSB) pursuant to the Bank Secrecy Act (BSA), regulations at 31 CFR 102.23(a)(2), administered by the Financial Crimes Enforcement Network (FinCEN).

Information contained on this site does not constitute an MSB registration. MSB registration is only conducted by FinCEN. Information provided on this site reflects only what was provided during its filing. Further information is available on the MSB. The registrant must follow the applicable regulations regarding a registration of Money Services Business (MSB) law.

MSB Registration Number: 200002004010
Registration Type: Initial Registration
Legal Name: null

Other Name:

Street Address: 1700 West Andrews Suite 800
City: Lakewood
State: CO 80123
Zip: 80123

MSB Activities:
Check number (including transfer's and money orders); Order in foreign exchange; Issue of money orders; Issue of transfer's checks; Money transfer; Sale of money orders; Sale of prepaid access; Sale of transfer's checks

States of MSB Number:

Alabama, Alaska, American Samoa, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, DC, Wisconsin, Wyoming, All States & Territories & Foreign Flag; All States/Territories

Number of Branches:
Authorized Signature Date: 05/12/2022
Revised Date: 05/12/2022

TECHNICAL SECURITY ASSESSMENT

HTML Source Code Analysis

Brand Impersonation

```
<title>Bitfinex</title>
```

- The site uses the legitimate "Bitfinex" brand name to appear authentic.

Fake Wallet/Payment System

```
<a href="/User/txcoin">  
  <span class="fzmm fcf">Retirar</span>  
</a>  
<a href="/User/index">  
  <span class="fzm fcch">Carteiras</span>  
</a>
```

- Proof of Missing Payment Infrastructure:
- No PCI-DSS compliant payment processors
- No Visa/Mastercard/Stripe/PayPal integration
- No bank transfer APIs
- No SSL security badges

Fake Financial Products

```
<a href="/Issue/index">  
  <span class="fzmm fcf">IEO</span>  
</a>  
<a href="/Orepool/index">  
  <span class="fzmm fcf">Staking</span>  
</a>  
<a href="/Contract/index">  
  <span class="fzmm fcch">Quick Margin</span>  
</a>
```

- Multiple sophisticated financial products claimed without corresponding technical implementation.

Fake Real-Time Data

```
function get_all_market_data(){  
  $.post("/Ajaxtrade/get_all_market_data", function(res){  
    // Fake price updates  
  });  
}  
setInterval("get_all_market_data()",50000);
```

- Proof: Simulated market data updates every 50 seconds without legitimate data sources.

Suspicious Service Worker

```
var serviceWorkerUri = '/ddos.js';  
navigator.serviceWorker.register(serviceWorkerUri)
```

- Service worker registration that could intercept and manipulate user data.

No Regulatory Compliance

Complete absence of:

- Legal documents (Terms of Service, Privacy Policy)
- Regulatory licenses display
- Company registration information
- Compliance badges

User Account Control

```
let userstatus=1;  
if(userstatus!=1){  
  layer.msg("Sua conta foi congelada. Entre em contato com o administrador");  
}
```

- Account freezing mechanism that forces victims to contact scammers.

AUTHENTICATION SYSTEM TESTING

Phase 1 — SQL Injection Assessment

A set of basic SQL injection payloads was used as part of a non-invasive assessment to confirm whether input fields exhibited classic SQL injection behavior. Example payloads used for validation (not exploitative) included common test strings such as: admin' OR '1'='1'-- and similar patterns.

Result: No exploitable SQL injection was identified during passive/limited testing.

Attempted SQL injection due to observed outdated system components, didn't work.

Phase 2 — Authentication Resistance Assessment

Limited credential-resistance checks were performed to evaluate whether the authentication subsystem resisted automated and credential-based attempts. These checks were restricted to observation of response behavior and non-destructive attempts; no personal data or sensitive information was accessed or retained.

Observed weaknesses (technical):

- No rate limiting: The authentication endpoints accepted multiple rapid attempts from the same source without effective throttling.
- No account lockout or progressive delay: Failed attempts did not trigger progressive delays or temporary account suspension.
- Weak credential validation: The system accepted weak/default passwords and did not enforce robust password policies.
- No bot mitigation: There was no CAPTCHA or comparable bot-challenge mechanism on the relevant flows.
- Single-factor authentication only: No multi-factor authentication (MFA) options were available.
- Session handling concerns: Session management did not demonstrably rotate or invalidate sessions upon sensitive events (observational finding).

Operator "ddos"/Admin Role Analysis

An account labelled ddos was observed in the service interface and is represented in the system as an "operator/admin"-style account. The observation was limited strictly to the account identifier and visible interface elements; no sensitive or personal data was accessed. Functionally, this account did not demonstrate elevated control over the platform beyond interacting with simulated/fake balances presented to users. In other words, even accounts presented as administrative appeared to have minimal real privileges and the site's backend functionality is largely superficial — reinforcing the conclusion that the platform is fraudulent and non-functional.

The authentication controls are insufficient for production use and present a credible risk for credential stuffing and automated abuse. No personal data was accessed or retained. Operational and exploitation details have been intentionally omitted for legal and safety reasons; responsible disclosure steps have been initiated.

Compromised Account Context:

- Username: ddos (technical/operational naming convention).
- Session State: Active operator session when accessed.
- Actual Role: Likely pyramid scheme recruiter/operator, not victim.
- Discovery Context: Part of multi-level fraud operation.

Administrative Hierarchy

REAL OPERATORS (hodt.xin backend)



OPERATORS LIKE "ddos" (Frontend recruiters)



VICTIMS WITH FAKE HIGH BALANCES (Active recruiters)



NEW VICTIMS (Bottom of pyramid)

Technical Evidence of Obscured Infrastructure:

Script Architecture Analysis:

JavaScript Void: Only jquery.min.js loads successfully - all other application scripts (main.js, app.js, common.js, custom.js, user.js) return 404 errors, indicating no functional client-side logic exists.

Directory Structure Revelations:

Blocked Access: Direct access to /Application/, /Controller/, /Model/, /View/ returns 403 Forbidden or ThinkPHP framework errors, confirming these are either non-functional or deliberately obscured.

Path Disclosure Evidence:

Internal Mapping: Error messages leak the internal server path /www/wwwroot/hodt.xin/ while publicly serving from cdfg.lat, demonstrating domain obfuscation.

Template System Failures:

Missing Components: The system attempts to load ./Application/Mobile/View/User/login.html but the template doesn't exist, revealing incomplete or fake MVC implementation.

Asset Isolation:

Limited Public Access: Only basic static assets in /Public/bendi/ and /Public/Static/ are accessible, while all dynamic endpoints and administrative paths lead to errors or redirections.

The technical investigation confirms a deliberately obscured structure where the public-facing site contains only superficial elements while all functional components are either missing or intentionally inaccessible.

THE DOCUMENT UPLOAD TRAP FOR WITHDRAWALS

A critical phase of the scam involves demanding document uploads for "verification" before allowing withdrawals.

The Mechanism

Victims are presented with a seemingly legitimate verification form requiring:

- Identification Document (ID Card/Passport)
- Proof of Address
- Selfie with Document

Possible Malicious Objectives

Identity Theft: Documents are harvested for use in bank fraud or to open accounts in the victims' names.

Creating Fake Profiles: Documents are used to verify other fraudulent accounts.



CONCLUSION & RESPONSIBLE DISCLOSURE

Executive Summary of a Sophisticated Fraud Network

"Operation Scam Hunter" has successfully identified, documented, and exposed a highly organized international financial fraud network. This investigation reveals a sophisticated operation designed to systematically defraud victims through a combination of social engineering, technical deception, and complex infrastructure.

Key Findings of the Network

Technical Infrastructure: A resilient and multi-layered infrastructure based on a central command panel (hodt.xin) and a rotating fleet of disposable front-end domains.

Fraudulent Methodology: A well-defined scam lifecycle, from luring with fake jobs to entrapping with fake investments and finally extracting documents for further extortion.

Proven Impact: Direct evidence from victim complaints confirms substantial financial losses and the harvesting of sensitive personal documents.

Immediate Action: Handover to Authorities and Platforms

In accordance with the principles of ethical hacking and responsible disclosure, the full intelligence package compiled during this investigation will be systematically disseminated to the relevant entities to facilitate actionable countermeasures.