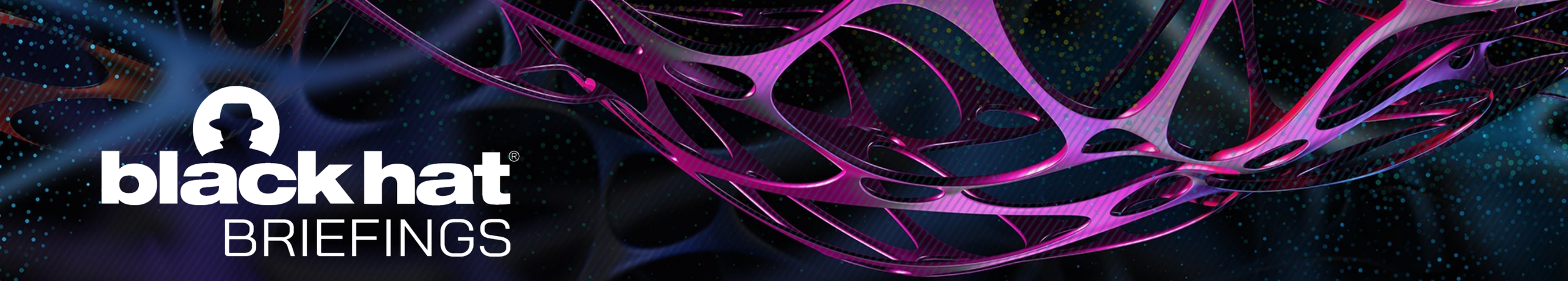


No Hoodies Here: Organized Crime in AdTech

Dr. Renée Burton
Dave Mitchell
Chris Kim

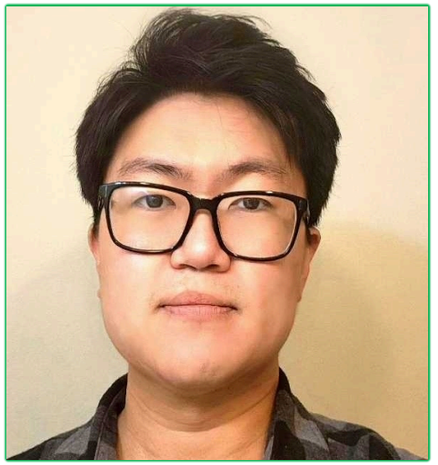
Infoblox Threat Intel

Who are we?

Infoblox Threat Intel

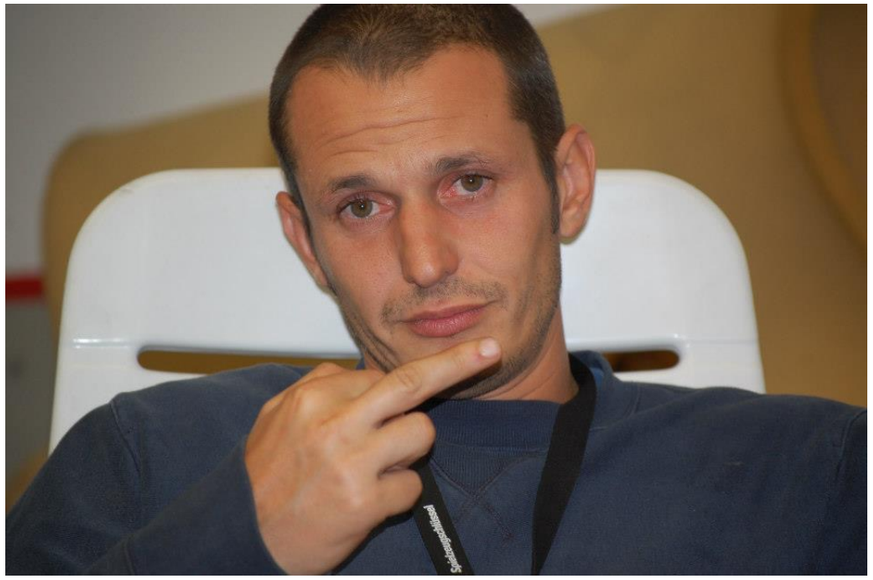
Renée Burton
VP of Infoblox Threat Intel

Dave Mitchell
Sr Director, Infoblox Threat Intel

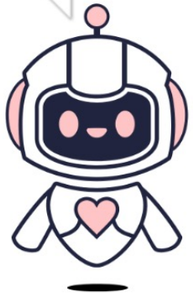


Chris Kim
Sr Staff Threat Researcher

Let's go on a journey into the world of malicious adtech...



7B9605E6-87A9-4F28-A134-C2F1A15C1FDD



youtube.com/watch?v=f_jBRq7Gd_Y

YouTube Search

Kroum Vassilev's Supersonic Flight to the Edge of Space

Kroum 21 subscribers Subscribe 4 Share Download Clip Save

210 views Apr 6, 2017

kroum • Follow
Switzerland

kroum Switzerland with good friends, always a winning combination. 🏔️❤️🇨🇭
248w

brendan_v_m Beautiful
248w 1 like Reply

chalashkanova 😍
248w 1 like Reply

lambojoe77 Breathtaking 👍🏻👍🏻👍🏻. Living your best lyfe 🙌🏻
248w 1 like Reply

ronirev Absolutely gorgeous there!
248w 1 like Reply

wilbursmithhh Sorry that I miss our dates last time Mr. lederhosen
248w 1 like Reply

anniecanale 🔥🔥🔥👌
248w 1 like Reply

199 likes
October 10, 2020

What do those images have in common?

We'll get there.

But first, a bit of background.

Advertising Platforms

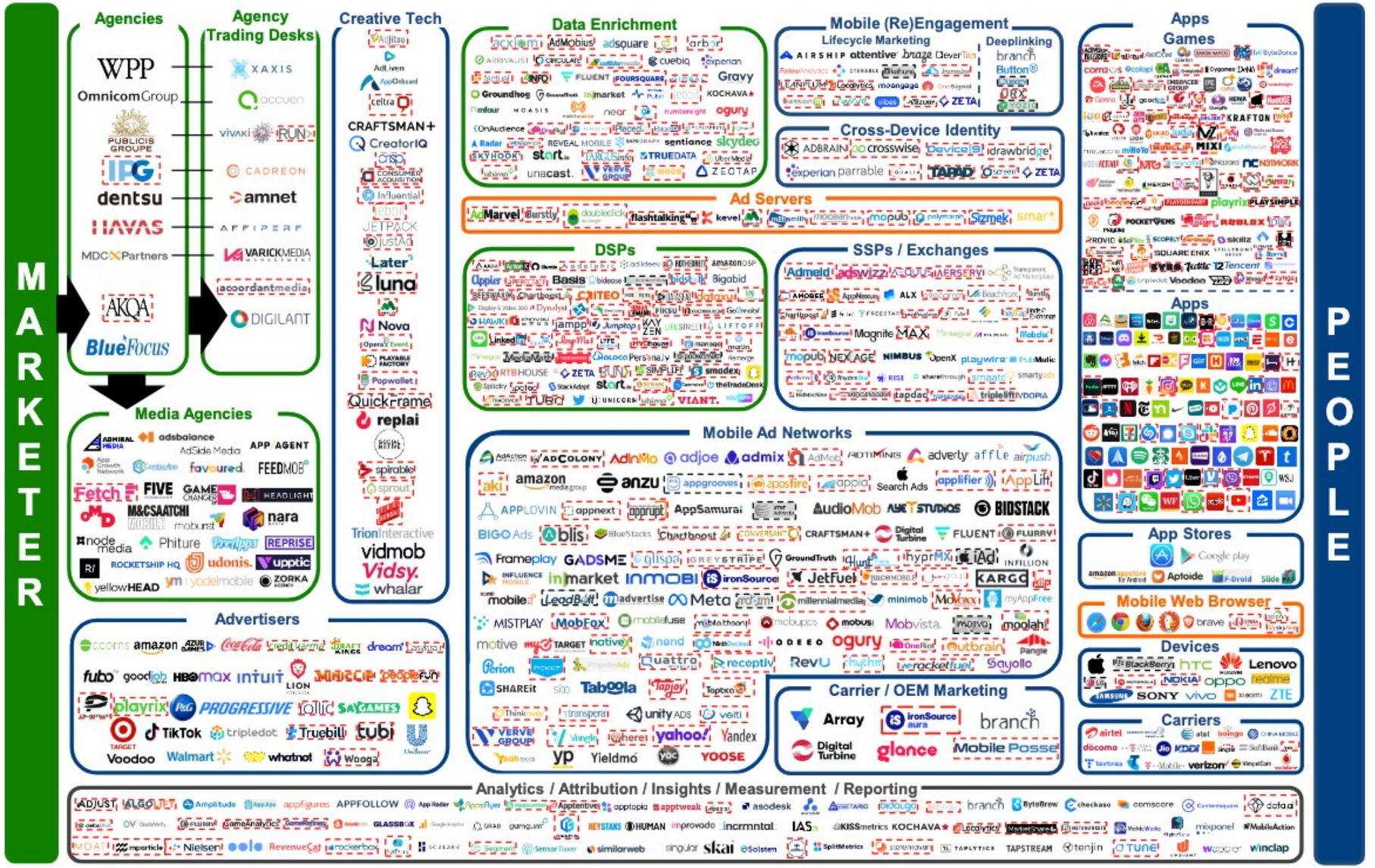
...are everywhere.

...are the financial backbone of the internet.

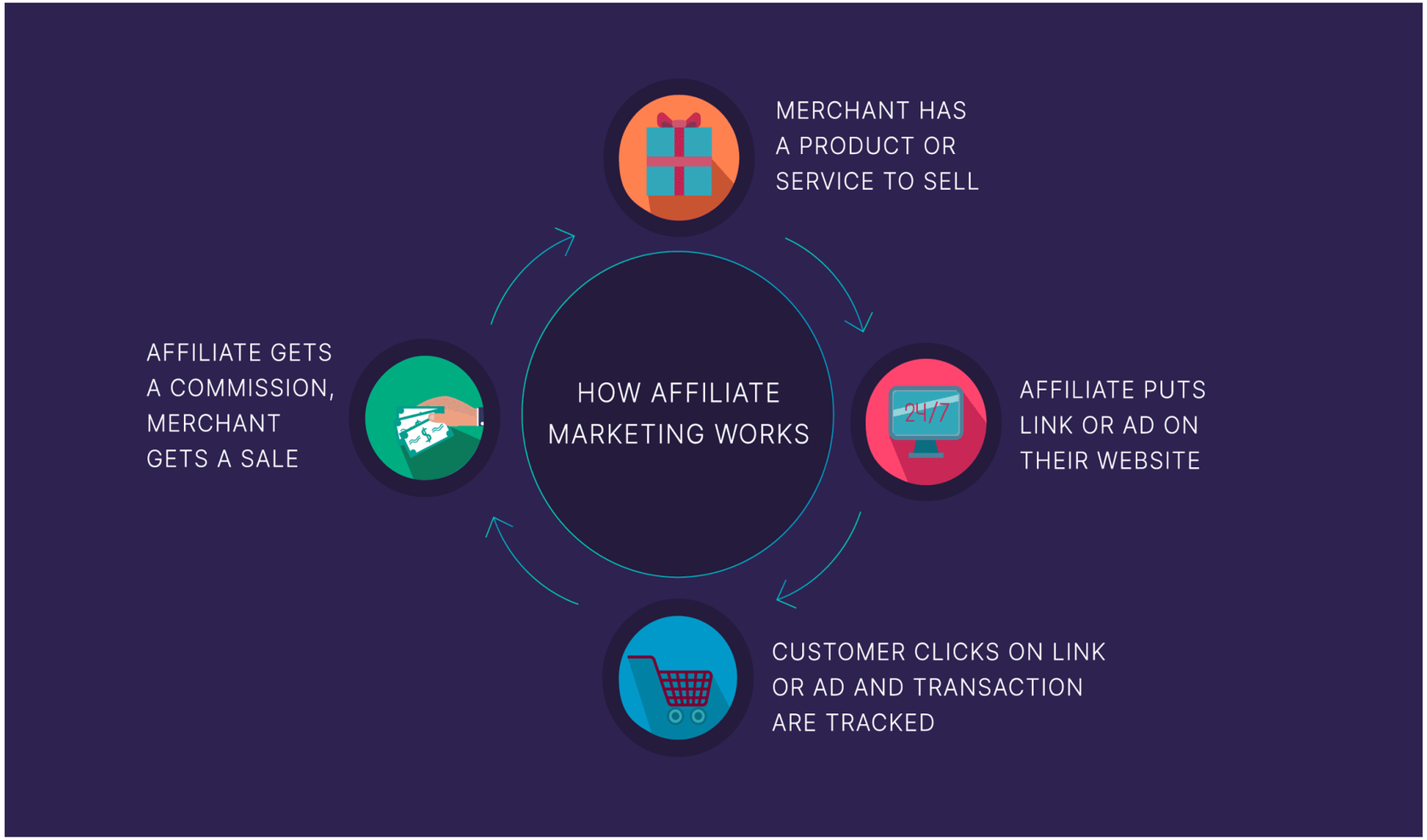
...are a great way for criminals to make a truckload of money.

...enable threat actors to distribute malware easily.

Mobile Ecosystem

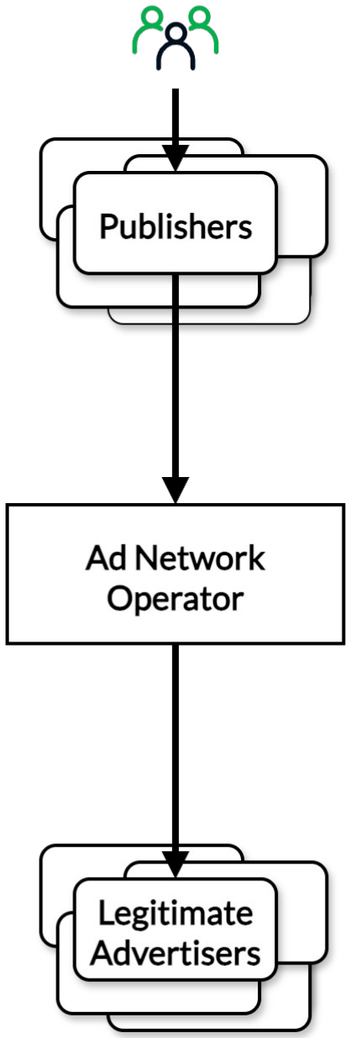


Affiliate Marketing



Legitimate vs. Malicious AdTech

Simplified Legitimate Adtech
(e.g., Google AdSense)



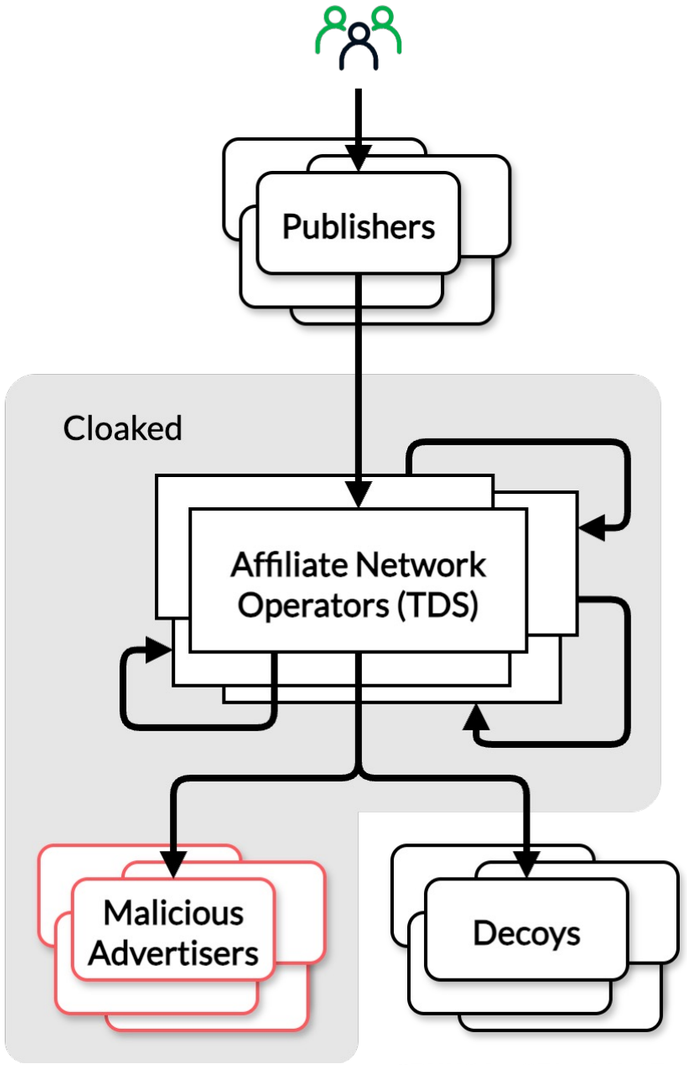
In malicious adtech, publishers can be network affiliates or affiliate network operators.

Traffic Distribution Systems (TDSs) are at the core of both legitimate and malicious ad networks. The TDSs cloak the network's infrastructure domains.

In malicious adtech, affiliates often use multiple affiliate networks and redirect between them.

In malicious adtech, advertisers are usually individual affiliates that target specific victim profiles. The landing pages are frequently cloaked to hinder investigations.

Simplified Malicious Adtech
(e.g., VexTrio Viper)



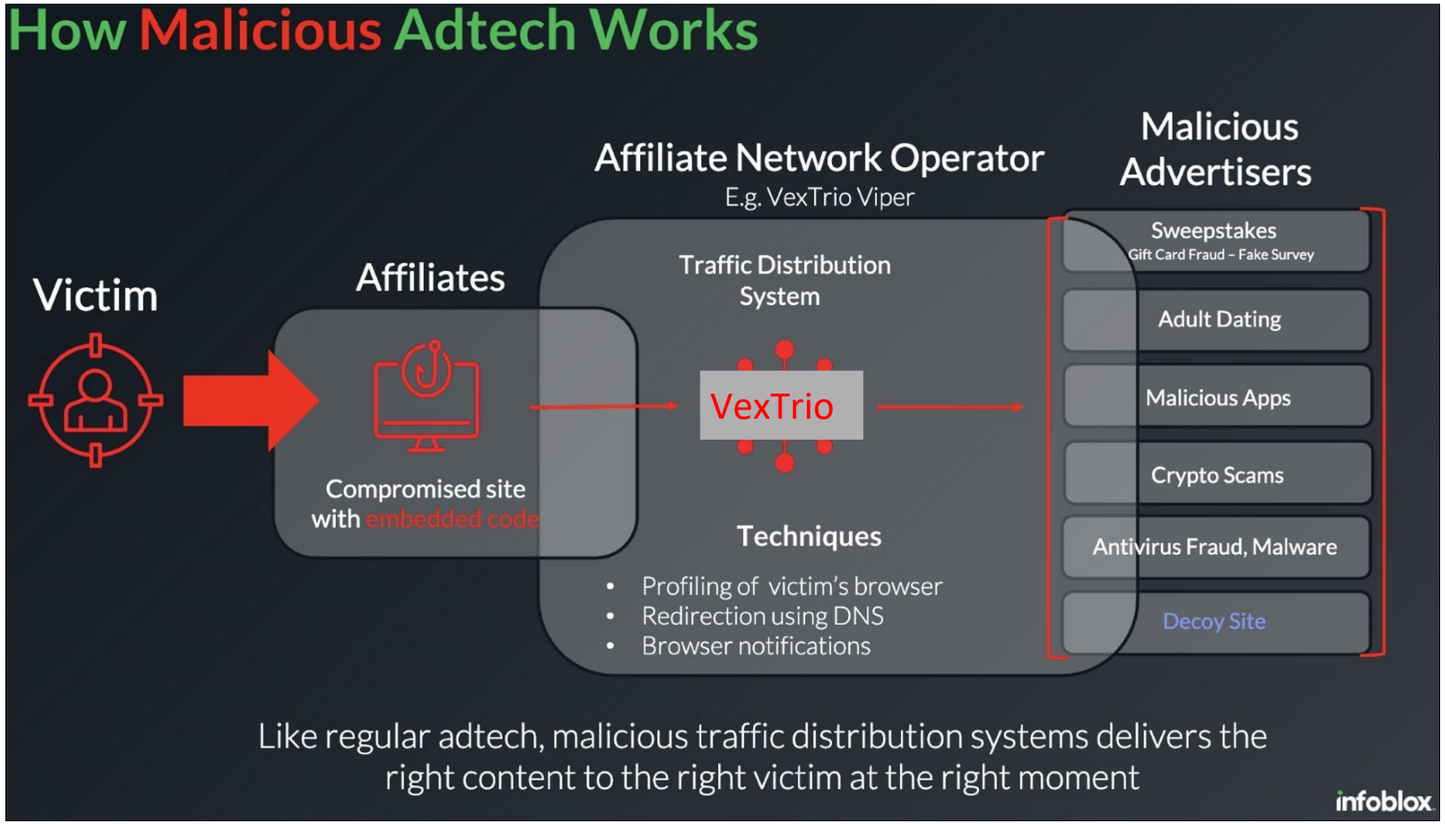
Enter VexTrio

Single largest TDS that is connected to compromised website redirections

Top 10k Popular Domains!

Nearly 40% of all compromised sites in 2014 redirected to VexTrio

We have observed in >50% of customer networks



VexTrio Affiliates with Bad Guys

VexTrio has a strong financial relationship with website hackers

- Transient relationships: SocGholish, ClearFake
- Long-time relationships: Balada Injector, DollyWay / Master134, Sign1, DNS TXT C2, Github SEO poisoner… more….

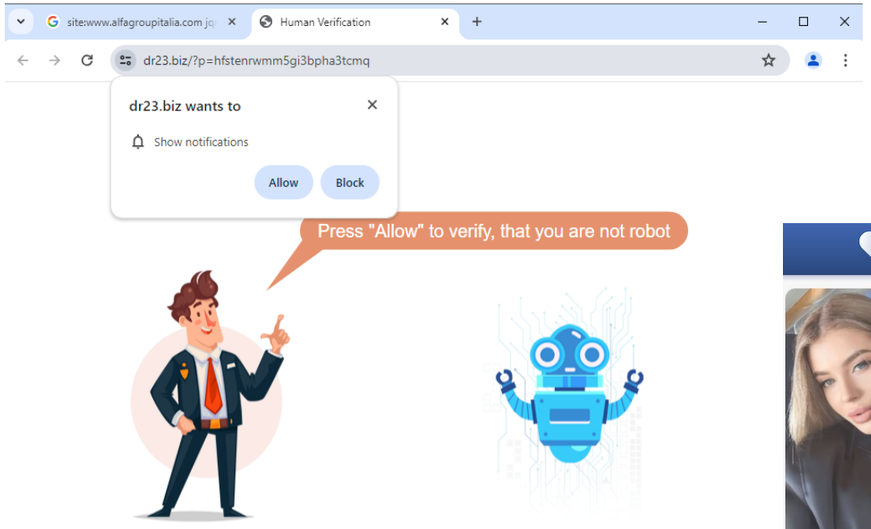
VexTrio TDS is intertwined with other notorious TDS: we suspect same actors

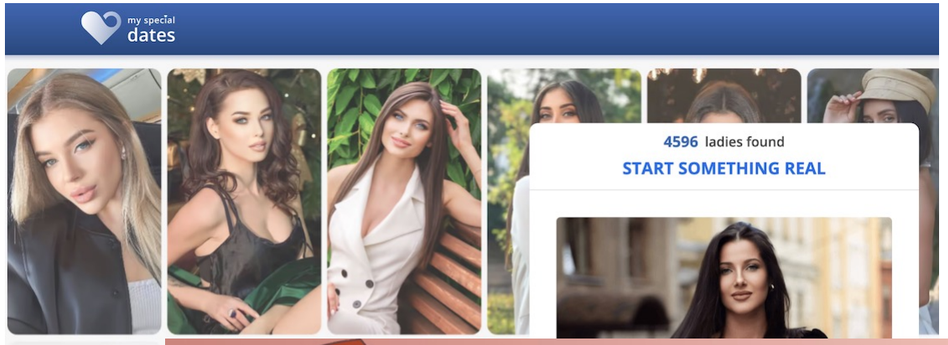
- Since at least 2017
- Help TDS, Disposable TDS, ROI777

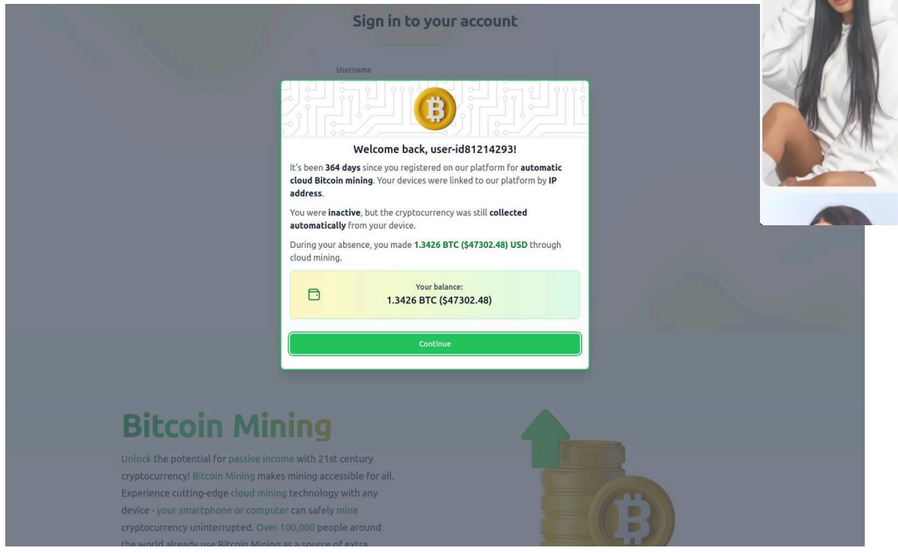
New research released June 13, 2025 on these relationships

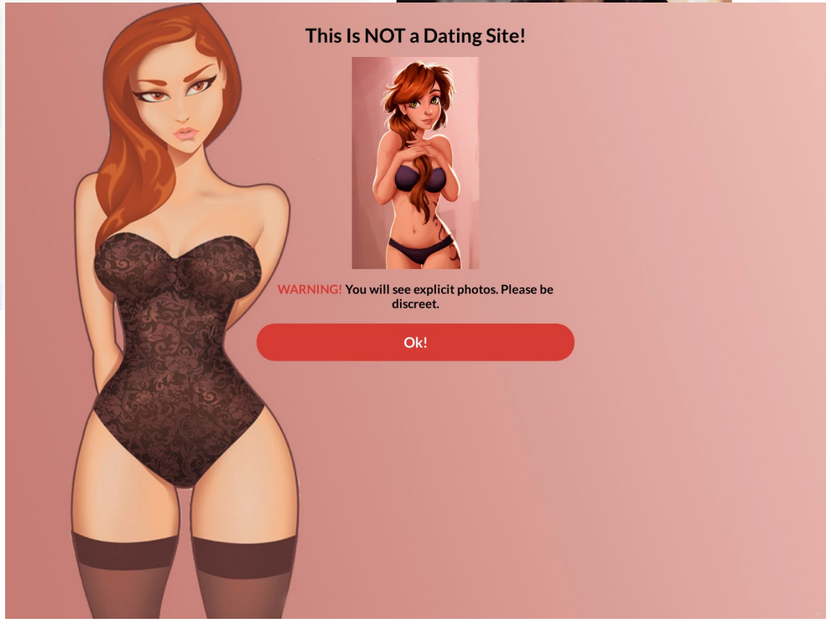
Have you or your loved ones been affected by one of these scams?

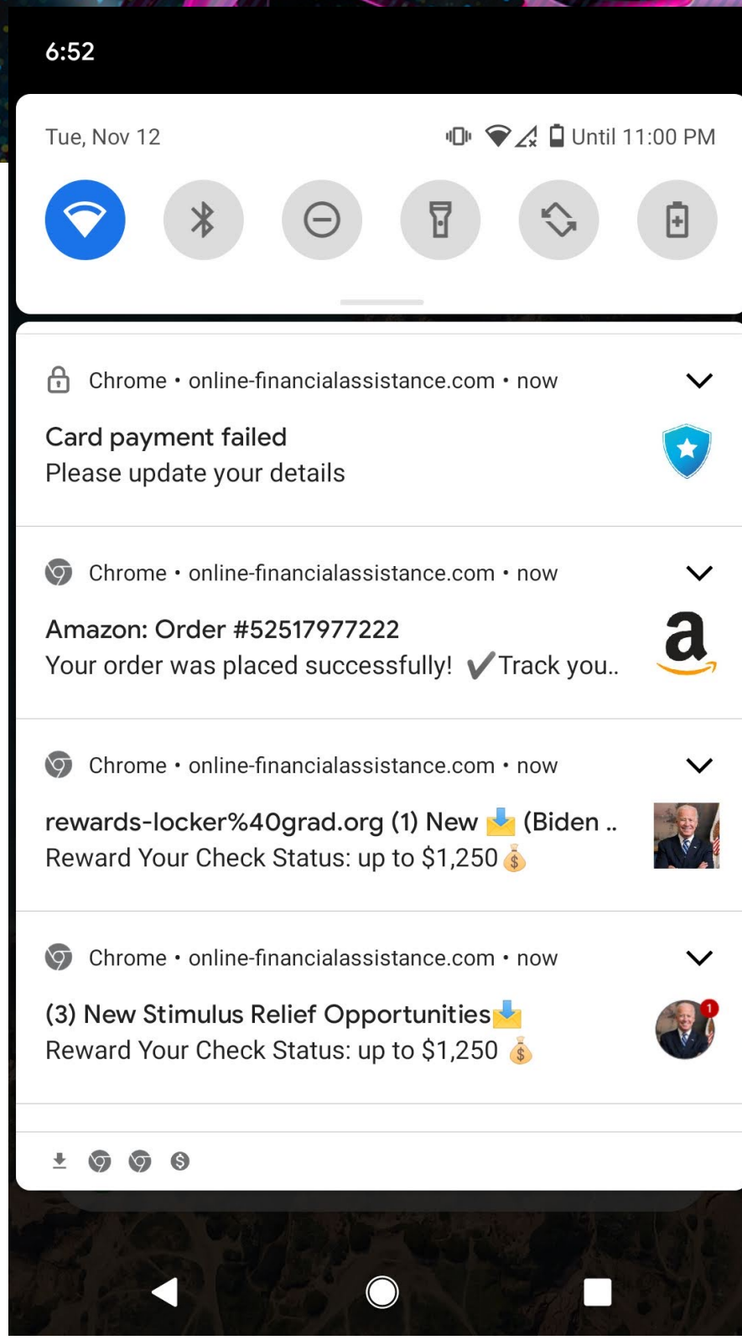
It was VexTrio.


site:www.alfagroupitalia.com jo
Human Verification
dr23.biz/?p=hfstenrwmm5gi3bpha3tcmq
dr23.biz wants to
Show notifications
Allow
Block
Press "Allow" to verify, that you are not robot


my special dates
4596 ladies found
START SOMETHING REAL


Sign in to your account
Username
Welcome back, user-id81214293!
It's been 364 days since you registered on our platform for automatic cloud Bitcoin mining. Your devices were linked to our platform by IP address.
You were inactive, but the cryptocurrency was still collected automatically from your device.
During your absence, you made 1.3426 BTC ($47302.48) USD through cloud mining.
Your balance:
1.3426 BTC ($47302.48)
Continue
Bitcoin Mining
Unlock the potential for passive income with 21st century cryptocurrency! Bitcoin Mining makes mining accessible for all. Experience cutting-edge cloud mining technology with any device - your smartphone or computer can safely mine cryptocurrency uninterrupted. Over 100,000 people around


This Is NOT a Dating Site!
WARNING! You will see explicit photos. Please be discreet.
Ok!


6:52
Tue, Nov 12
Until 11:00 PM
Chrome • online-financialassistance.com • now
Card payment failed
Please update your details
Chrome • online-financialassistance.com • now
Amazon: Order #52517977222
Your order was placed successfully! ✔Track you..
Chrome • online-financialassistance.com • now
rewards-locker%40grad.org (1) New (Biden ..
Reward Your Check Status: up to $1,250
Chrome • online-financialassistance.com • now
(3) New Stimulus Relief Opportunities
Reward Your Check Status: up to $1,250

Google Play

Your results indicate your phone may have adware installed, or be victim of spam-sending websites.

Proceed to clean and secure your phone with Spam Lock, on a 100% free 7 day trial – internet-only offer.

Next

MR BEAST

MEGA CHALLENGE FROM MR. BEAST

GET FROM 0.001 TO 1 BITCOIN FROM THE POPULAR YOUTUBE BLOGGER MR. BEAST

SENT TO SUBSCRIBERS
26.740 BTC

PARTICIPATE IN THE CHALLENGE FROM MR. BEAST

SUBSCRIBE SUBSCRIBE SUBSCRIBE

Hi guys! I, Mr. Beast, am starting another challenge today.
Today I will give away 30 Bitcoin to of my subscribers.
Anyone can take part.
How to take part in the challenge from Mr. Beast?

- Submit an application to participate in the challenge.
- Subscribe to my YouTube channel.
- Subscribe to my Instagram.
- Subscribe to my Tik Tok.

* Participants and a prize amount will be randomly selected.

Google Security
Saturday
9 November 2024

WARNING! Your is severely damaged by 13 Malware!

We have detected that your is (62%) DAMAGED by Tor.Jack Malware. Malicious and Aggressive Ads have injected this on your device.
Immediate Action is required to Remove and Prevent it from spreading that will leak sensitive data from your device. It includes your Social Media Accounts, Messages, Images, Passwords, and Important Data.

Here is how you can solve this easily in just a few seconds.

Step 1: Click the button below, "Allow error alerts," then subscribe to recommended spam protection app on the next page.

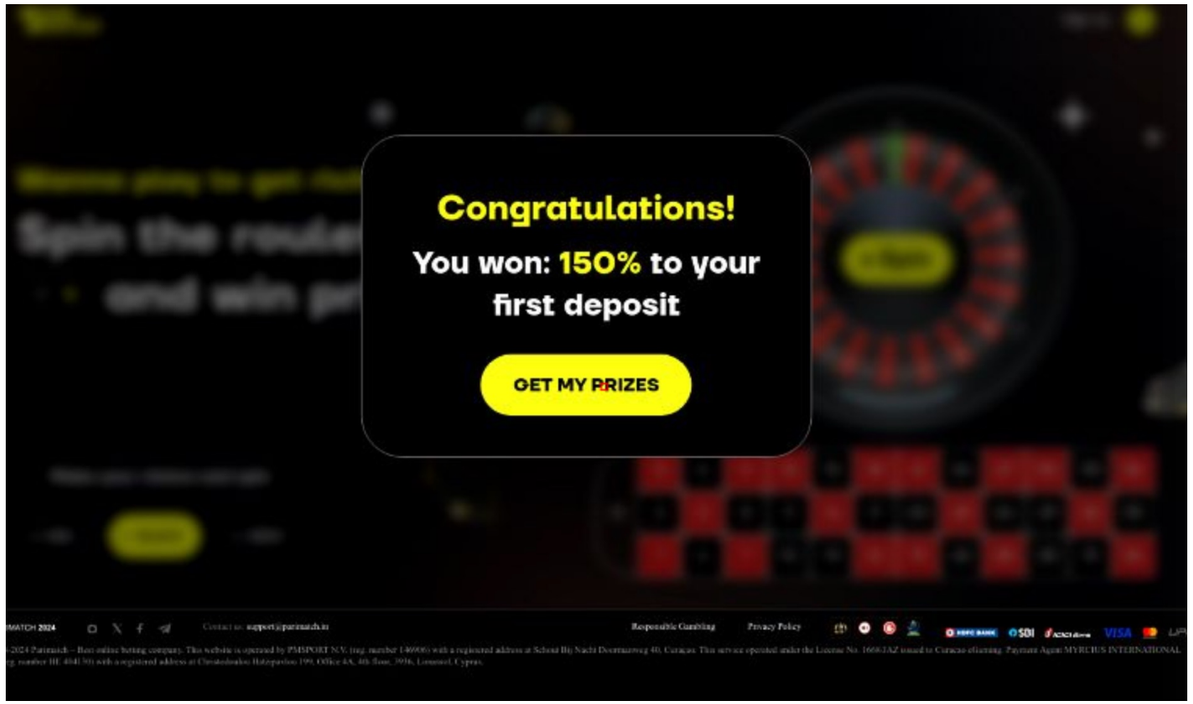
Step 2: Run the powerful Google Play-approved application to clear your phone from SPAM ads and block potential Malware with a few taps.

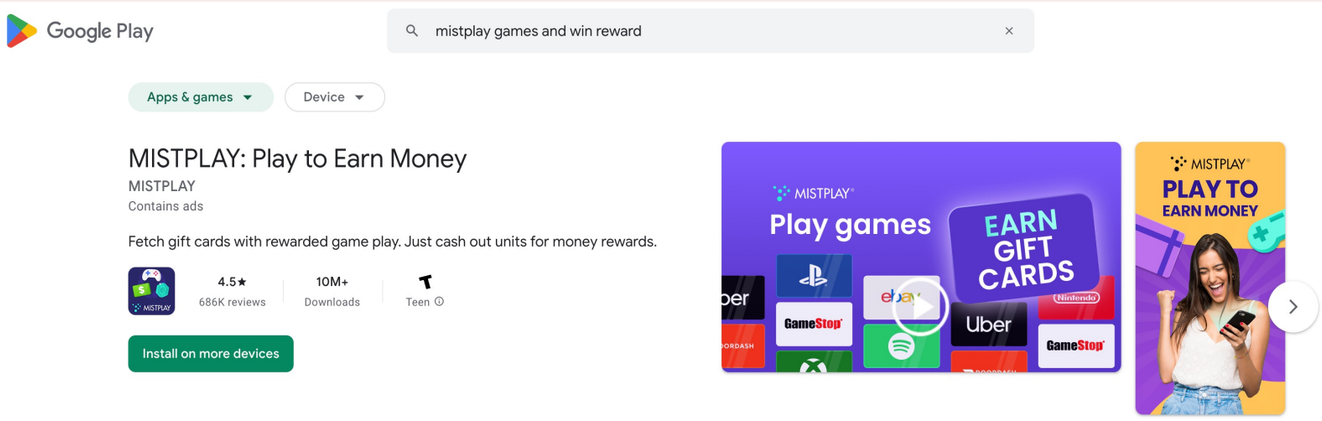
Clean my Device

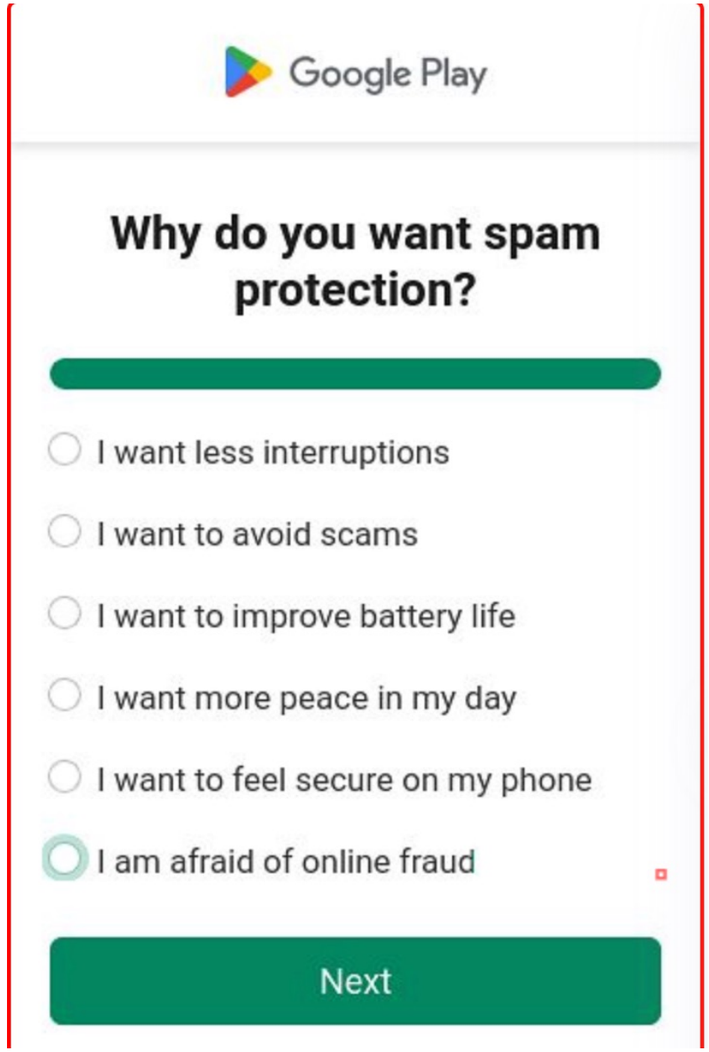
Detected By: Google

YOUR DEVICE HAS BEEN COMPROMISED!
Immediate Action is Required!

OK


Congratulations!
You won: 150% to your first deposit
GET MY PRIZES

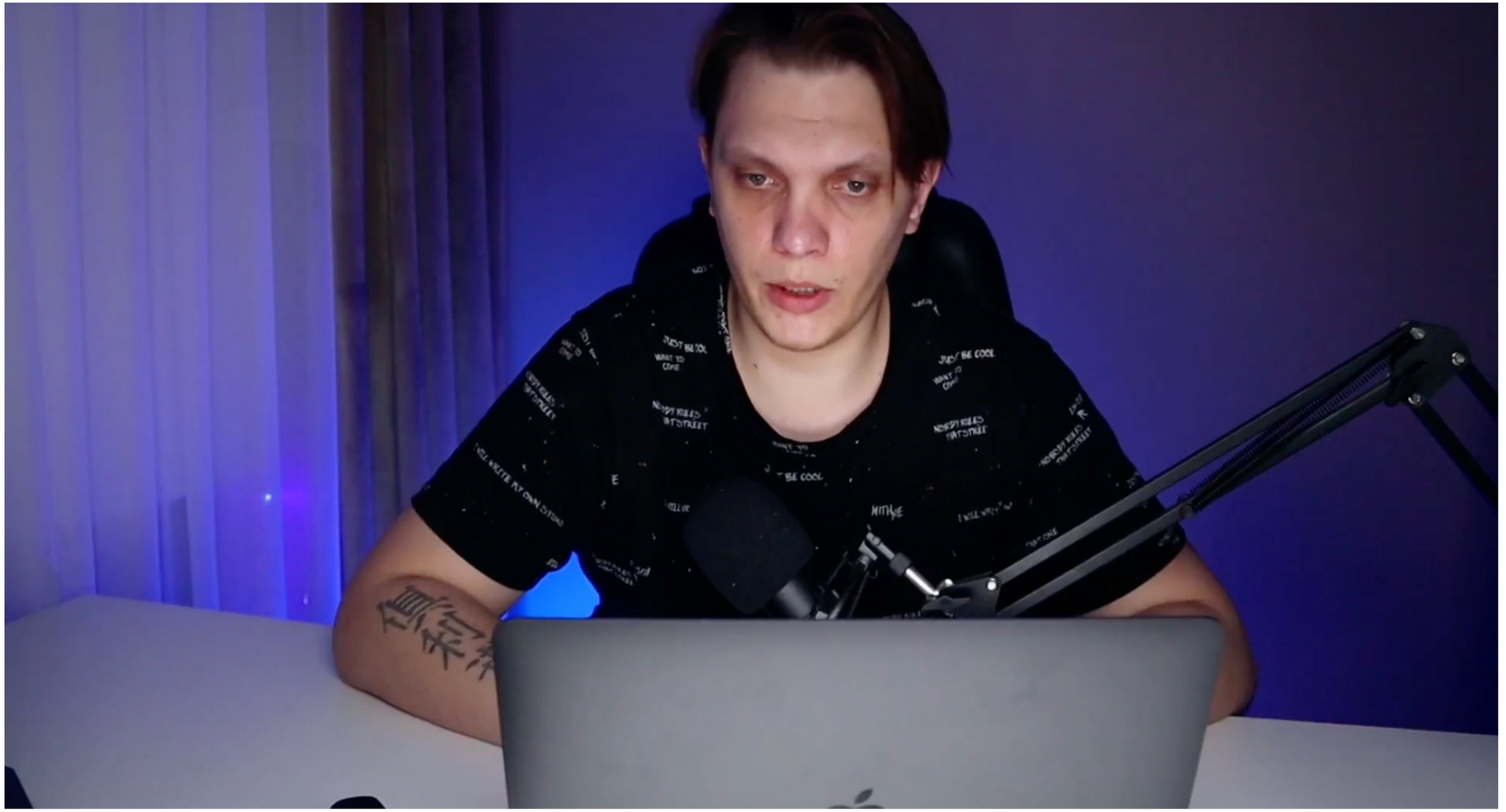

Google Play
mistplay games and win reward
Apps & games
Device
MISTPLAY: Play to Earn Money
MISTPLAY
Contains ads
Fetch gift cards with rewarded game play. Just cash out units for money rewards.
4.5★
686K reviews
10M+
Downloads
Teen
Install on more devices
MISTPLAY
Play games
EARN GIFT CARDS
Uber
GameStop
MISTPLAY
PLAY TO EARN MONEY


Google Play
Why do you want spam protection?
I want less interruptions
I want to avoid scams
I want to improve battery life
I want more peace in my day
I want to feel secure on my phone
I am afraid of online fraud
Next

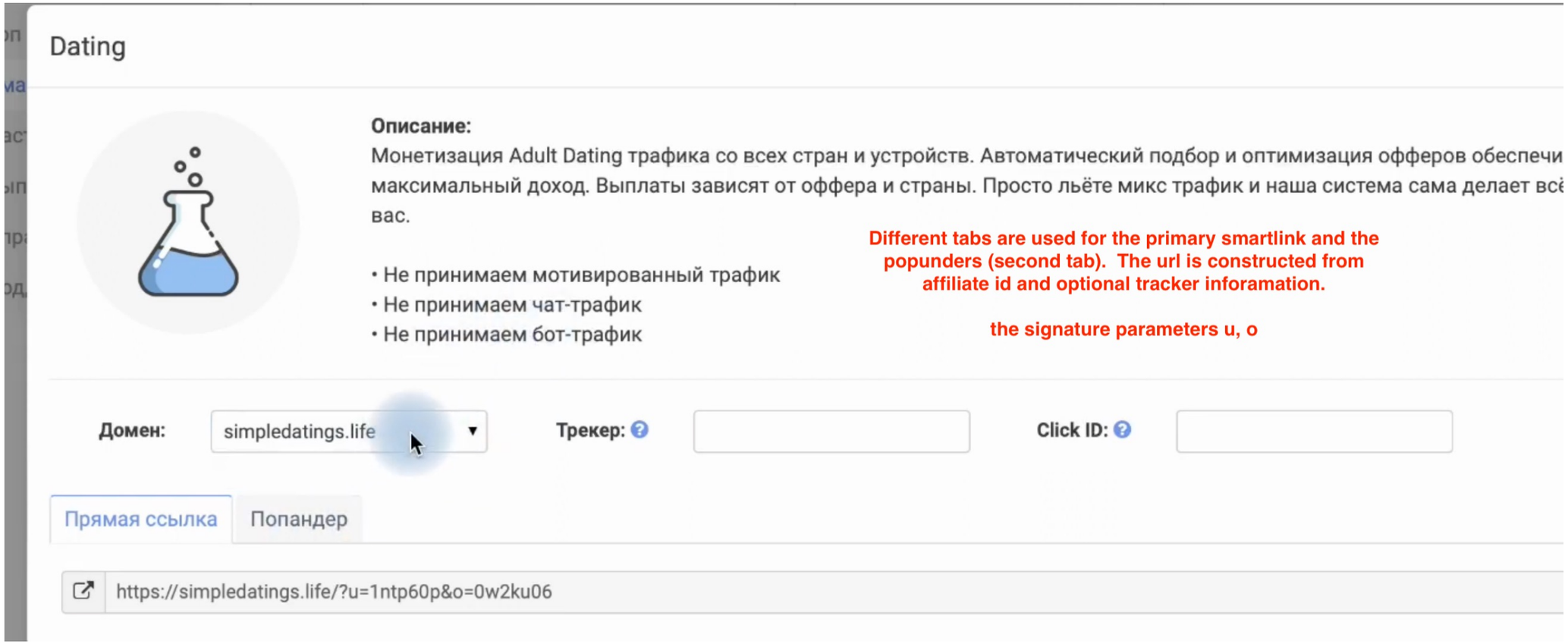
Our big break!

Years of frustration cured by a single frame of a YouTube video.

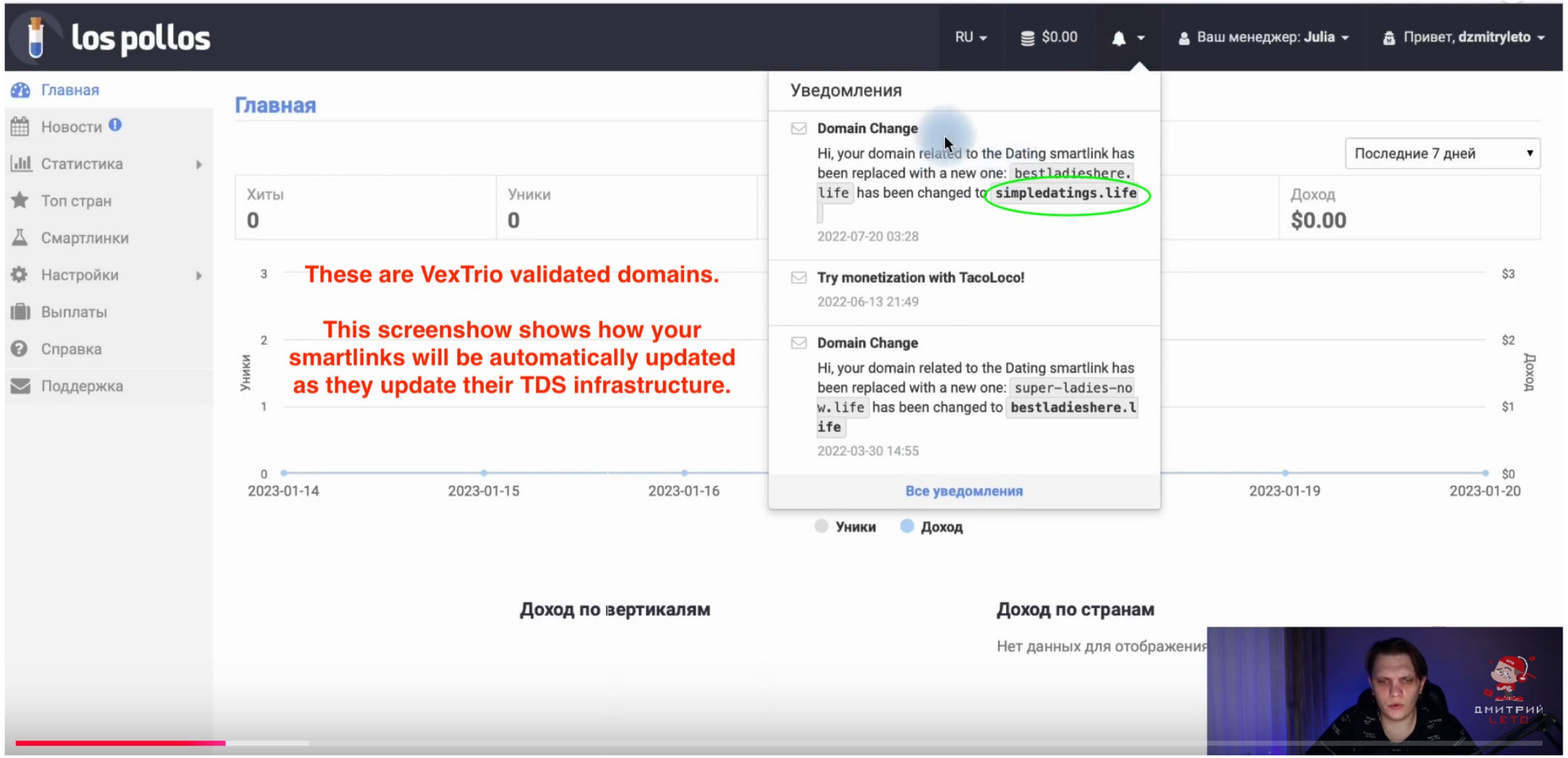
All about CPA marketing – in Russian



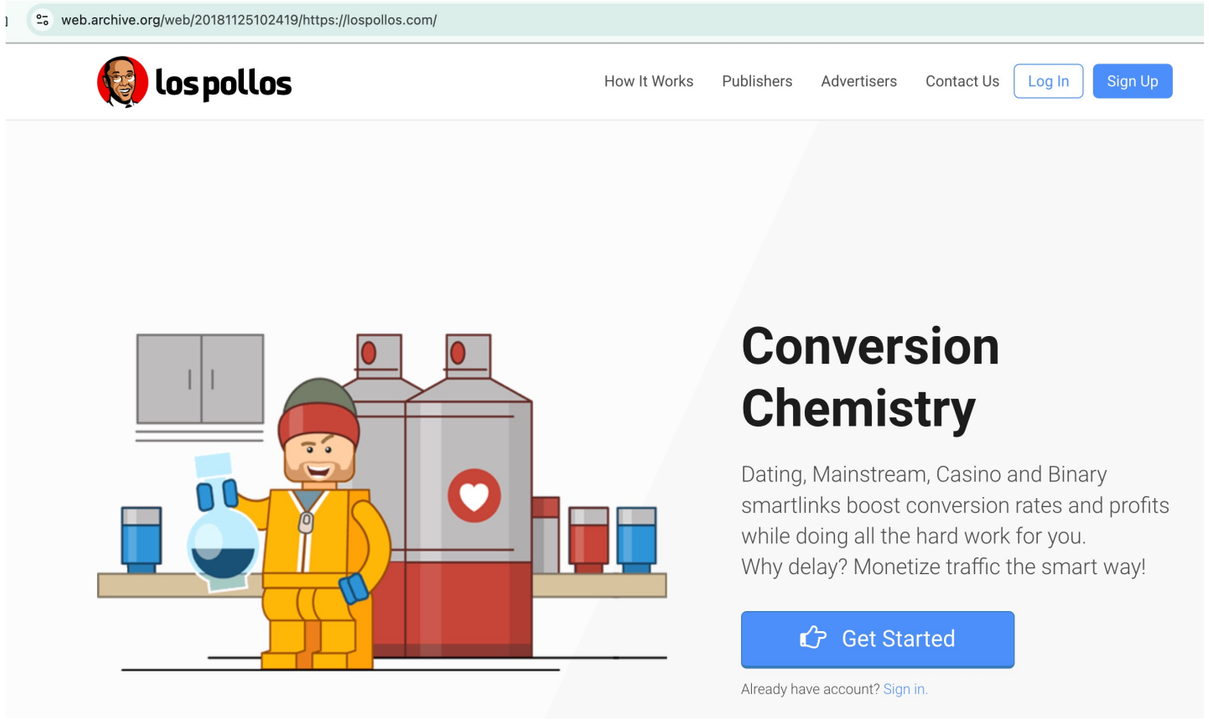
Bazinga – the VexTrio URL format

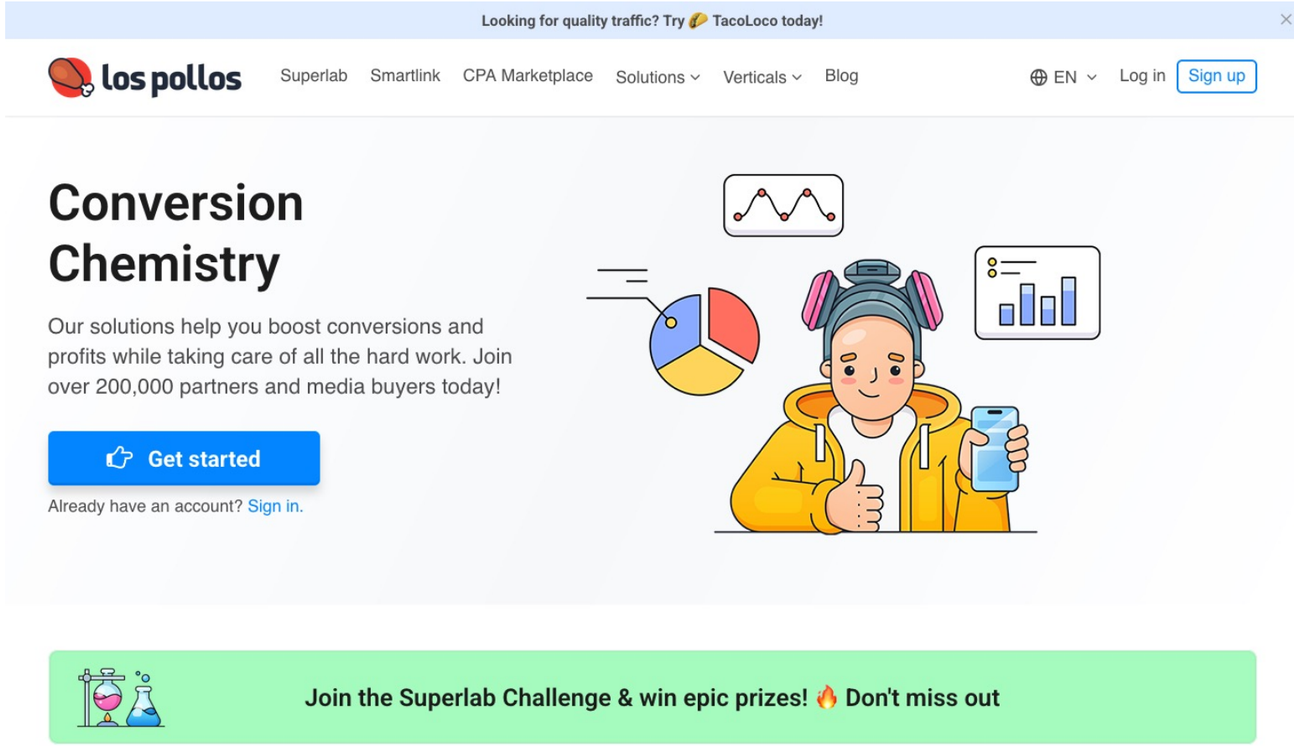


Los Pollos!

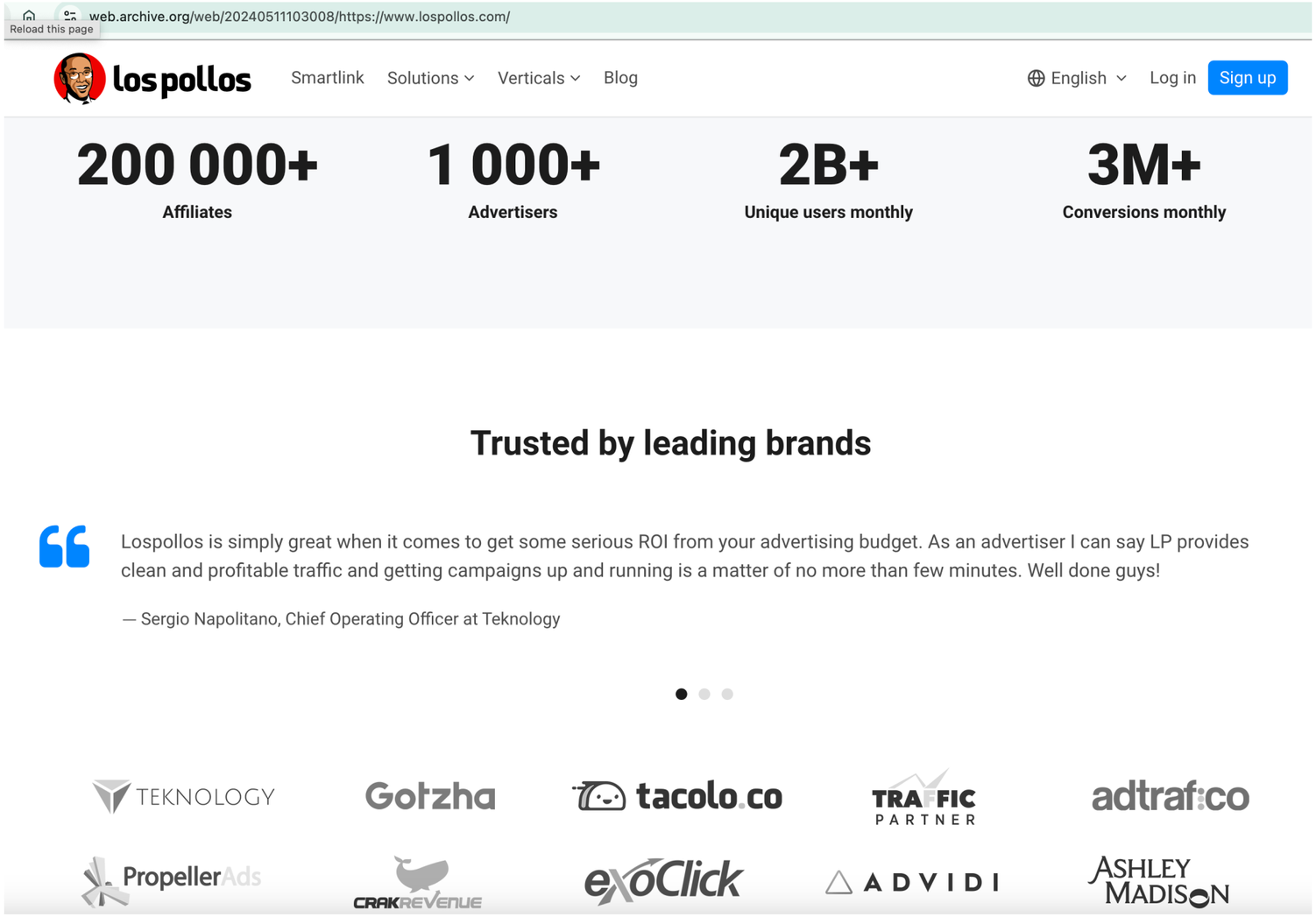

los pollos
RU
$0.00
Ваш менеджер: Julia
Привет, dzmitryleto
Главная
Новости
Статистика
Топ стран
Смартлинки
Настройки
Выплаты
Справка
Поддержка
Главная
Последние 7 дней
Хиты
0
Уники
0
Доход
$0.00
These are VexTrio validated domains.
This screenshow shows how your smartlinks will be automatically updated as they update their TDS infrastructure.
Уведомления
Domain Change
Hi, your domain related to the Dating smartlink has been replaced with a new one: bestladieshere.life has been changed to simpledatings.life
2022-07-20 03:28
Try monetization with TacoLoco!
2022-06-13 21:49
Domain Change
Hi, your domain related to the Dating smartlink has been replaced with a new one: super-ladies-now.life has been changed to bestladieshere.life
2022-03-30 14:55
Все уведомления
Уники
Доход
2023-01-14
2023-01-15
2023-01-16
2023-01-19
2023-01-20
Доход по вертикалям
Доход по странам
Нет данных для отображения
ДМИТРИЙ ЛЕТО

Breaking Bad. Fitting for VexTrio.

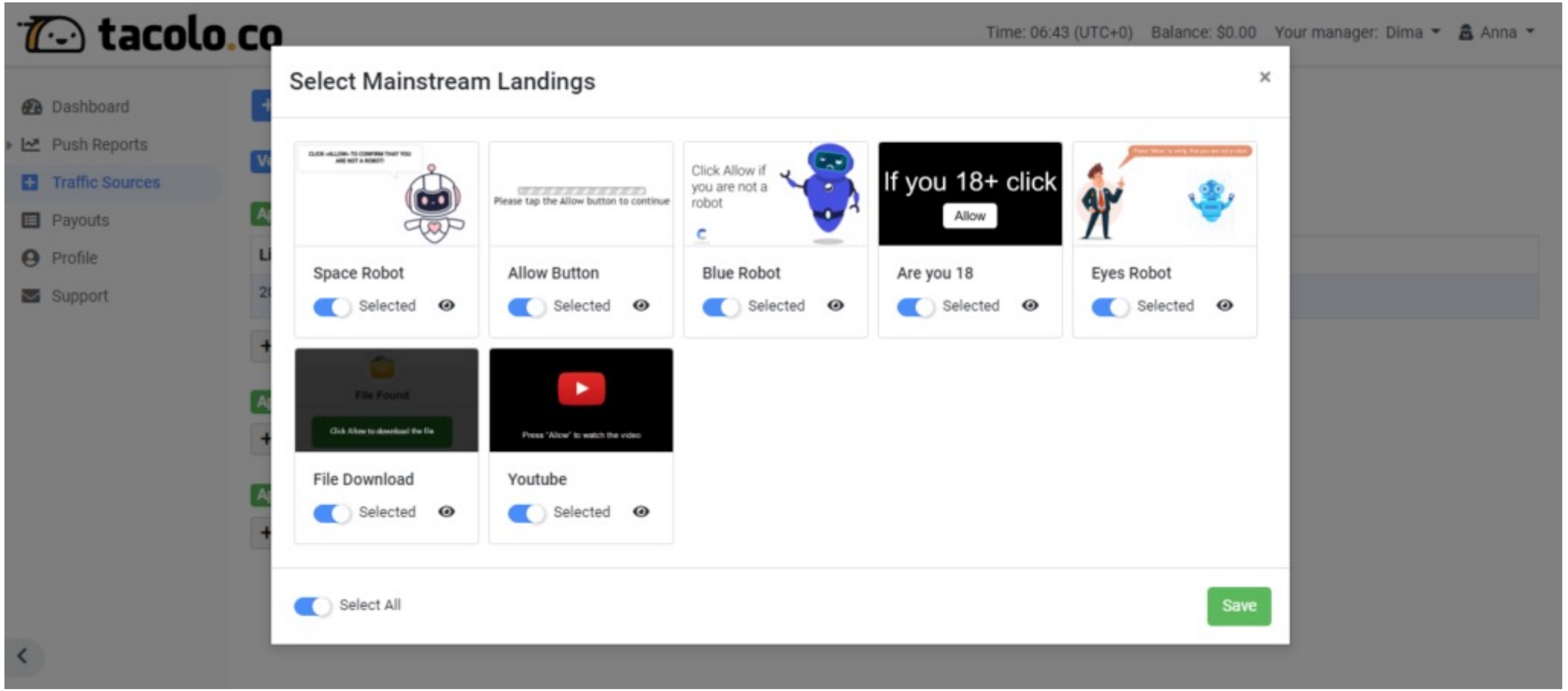




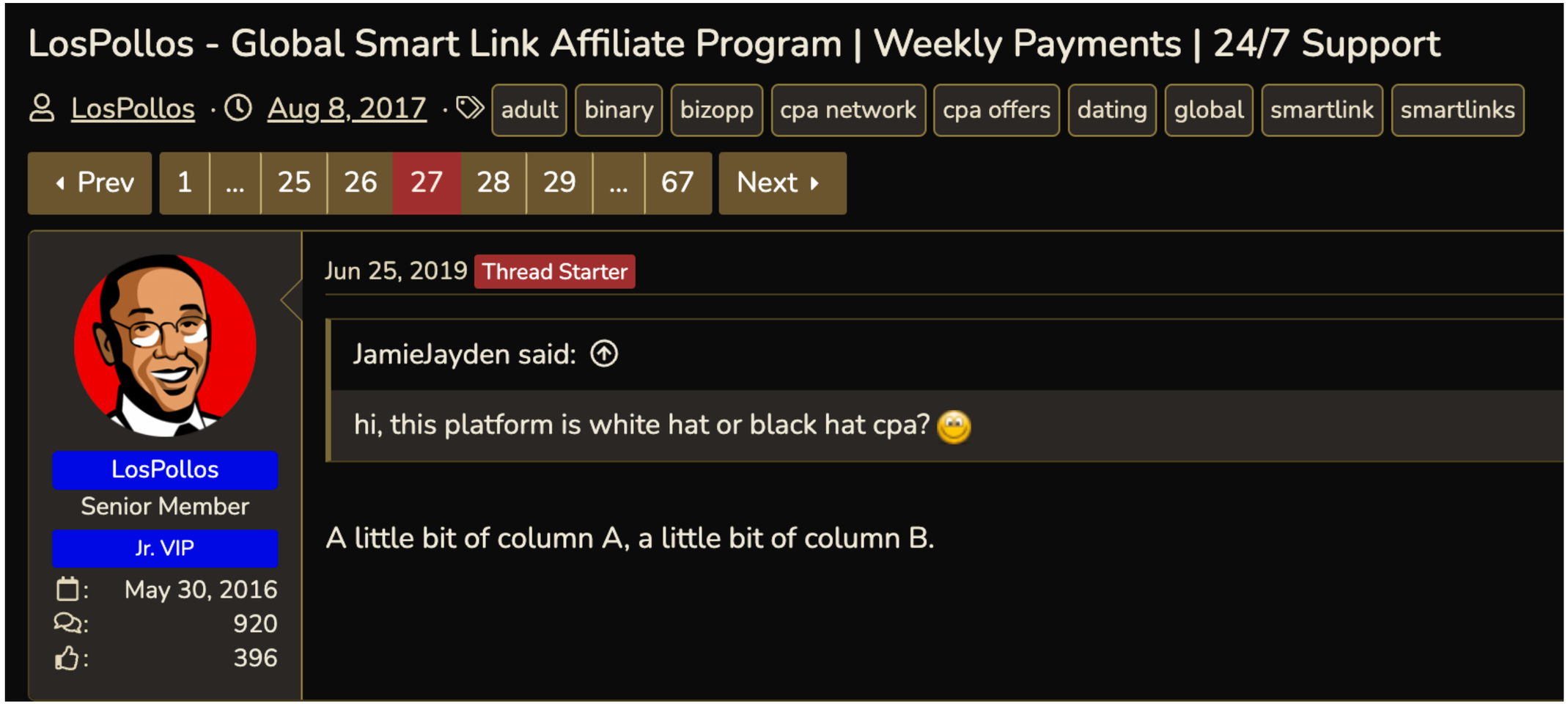
Turns out some of these companies are one in the same...



Yup, these guys.

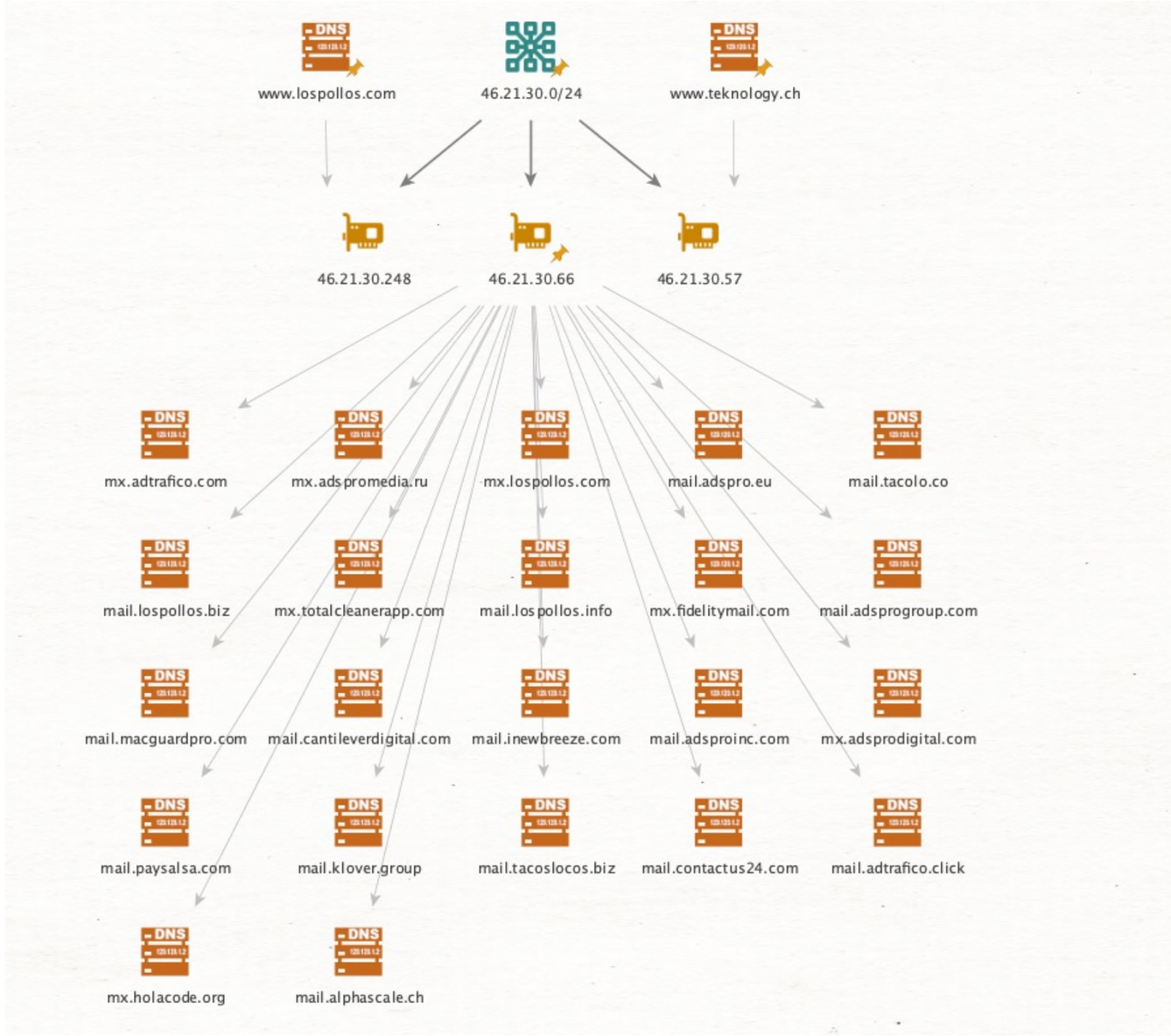


A little white hat, a little black hat CPA



Passive DNS Ties

All on one /24:
- Los Pollos
- Taco Loco
- AdTrafico
- ***AdsPro Group / AdsPro***
- ***Teknology***
- ***Holacode***
- Alphascale
- PaySalsa
- Fidelity Mail
- Cantilever Digital
- Klover Group
- Total Cleaner App



All Roads Lead to AdsPro

We are Adspro Group

We transform ideas into competitive startup ecosystems and create innovative solutions for AdTech products.

View careers 6

We create Internet services

Adspro develops unique services and complex solutions for AdTech and MarTech projects. We create own proprietary SaaS platform and unique services for international audience.

Read more about us

web.archive.org/web/20241120050039/https://www.adspro.eu/

We take on the most

Our team consists of creative experts with a thirst for discovery. We believe that for talented and progressive people there are no limits and boundaries.

Look at our global offices

Solutions and partners we rely on

We trust in a carefully selected range of innovative solutions and reliable partners to deliver exceptional results

tacolo.co

TacoLoco, the innovative ad network, efficiently processes over 1 million requests per second, delivering revolutionary performance for advertisers.

tacolo.co

lospollos

Marketing platform delivers over 3 million conversions per month. Advanced data analysis algorithms select the best CPA offers integrated into smartlink.

lospollos.com

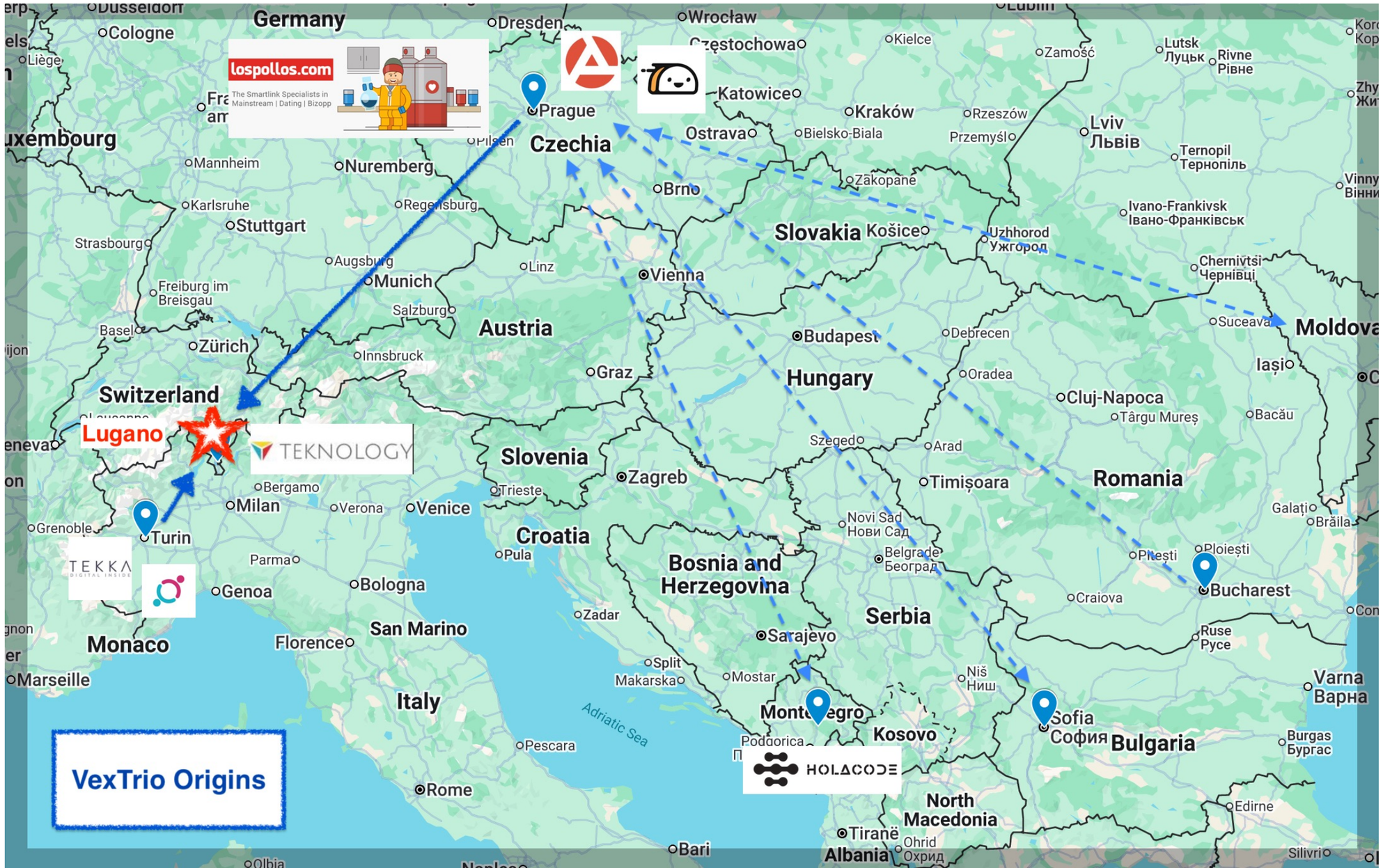
adtrafico

Adtrafico, a highly reputable leading performance marketing network, offers a vast selection of high-converting offers from hundreds of global advertisers.

adtrafico.com

Everyone Loves a Good Origin Story

Thank You, Internet.

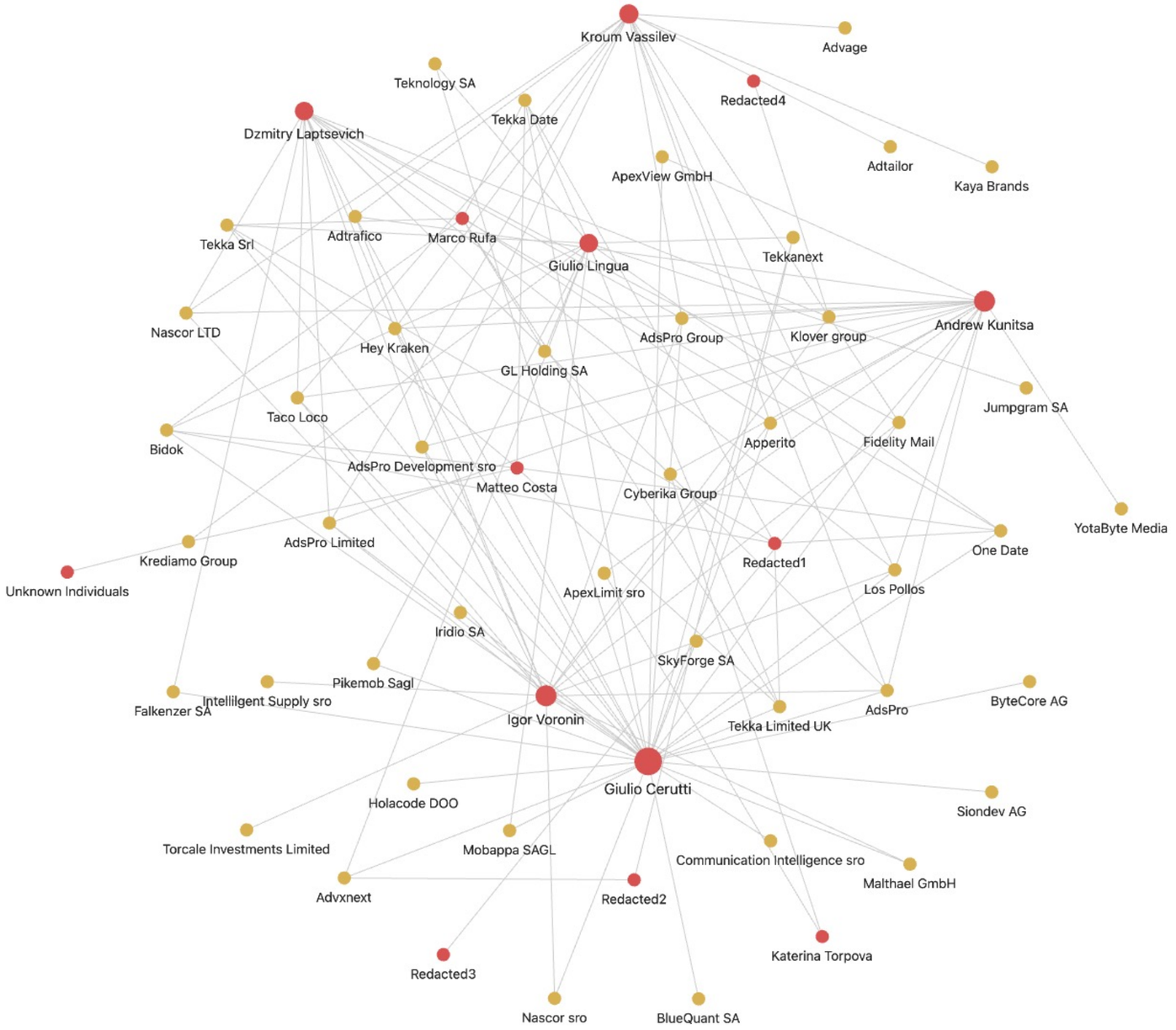


Two major groups:

- Italian (Turin)
- Russian speakers

- Origin story back to ~2004

- Merger ~2020 in Lugano



Pulling Thread

Dozens of micro-companies across a dozen countries

8-10 key figures

Hard find the boundary between companies and partners

The Italians

More Italians – business guys

businessmonitor

Prospect Lists | Company Search

Marco Rufa

Involvement

VICE-PRESIDENT

Fiduciaria Ferrecchi SA

MEMBER OF THE BOARD OF DIRECTORS

Marlu SA

Alumetal International SA

ETC Exclusive Travel Consulting SA

Intermetall Produkte AG

Centro Tosaerba e Giardinaggio SA

GL HOLDING SA

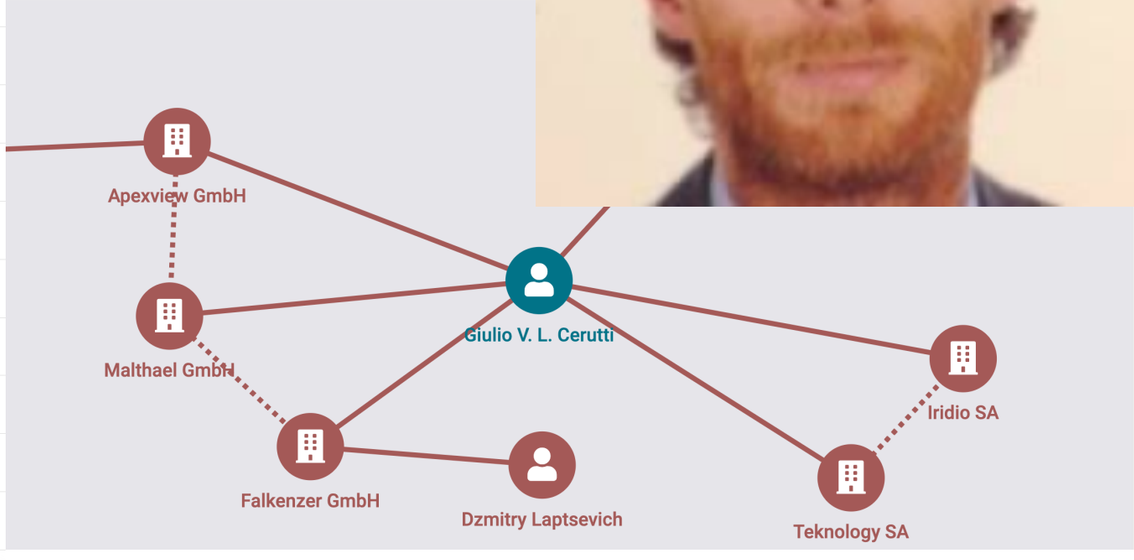
HPL INVEST SA

HFV Europe SA

SYNTEG SA

Amgest SA

SIGIT PROMOTERS SA



The Eastern Europeans

some are good at hiding…

others not so much…

kroum • Follow
Switzerland

kroum Switzerland with good friends, always a winning combination. 🙏❤️🇨🇭
248w

brendan_v_m Beautiful
248w 1 like Reply

chalashkanova 😍
248w 1 like Reply

lambojoe77 Breathtaking 👍👍👍. Living your best lyfe 🙌
248w 1 like Reply

ronirev Absolutely gorgeous there!
248w 1 like Reply

wilbursmithhh Sorry that I miss our dates last time Mr. lederhosen
248w 1 like Reply

anniecanale 🔥🔥🔥👌
248w 1 like Reply

199 likes
October 10, 2020

Igor Itpark is 😉 feeling grateful with **Mari Li** and **Olga Kunitsa** at **Klausenpass**.
September 27, 2020 · Unterschächen, Switzerland ·

Atlantic road trip 😎

New Friends!

K

Kevin Mccalister

Студент(ка) в уч. заведении University of Oxford

Rome, Latium, Italy · Contact info

University of Oxford

Connect | View in Recruiter | More

Activity

0 followers

Kevin hasn't posted yet

Recent posts Kevin shares will be displayed here.

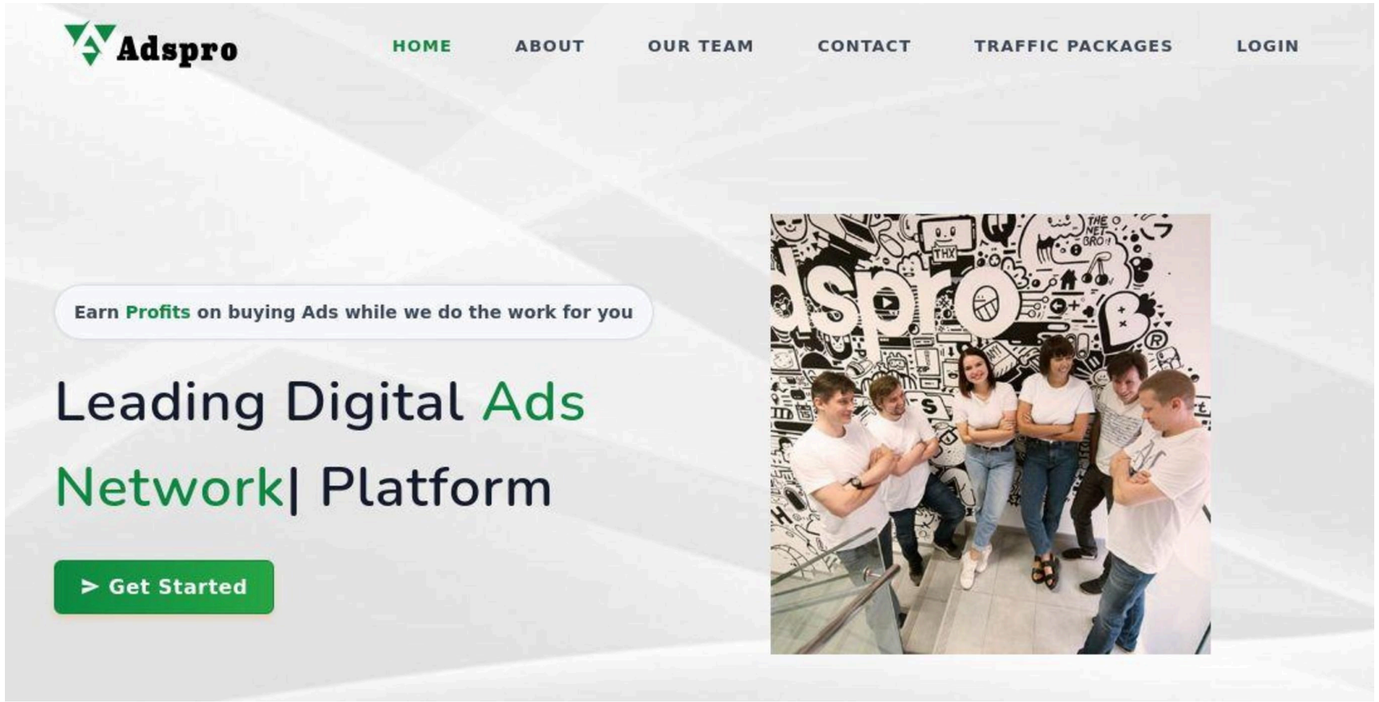
Show all activity →

Education

University of Oxford

2020 - 2030

The Disappearing Internet Archive

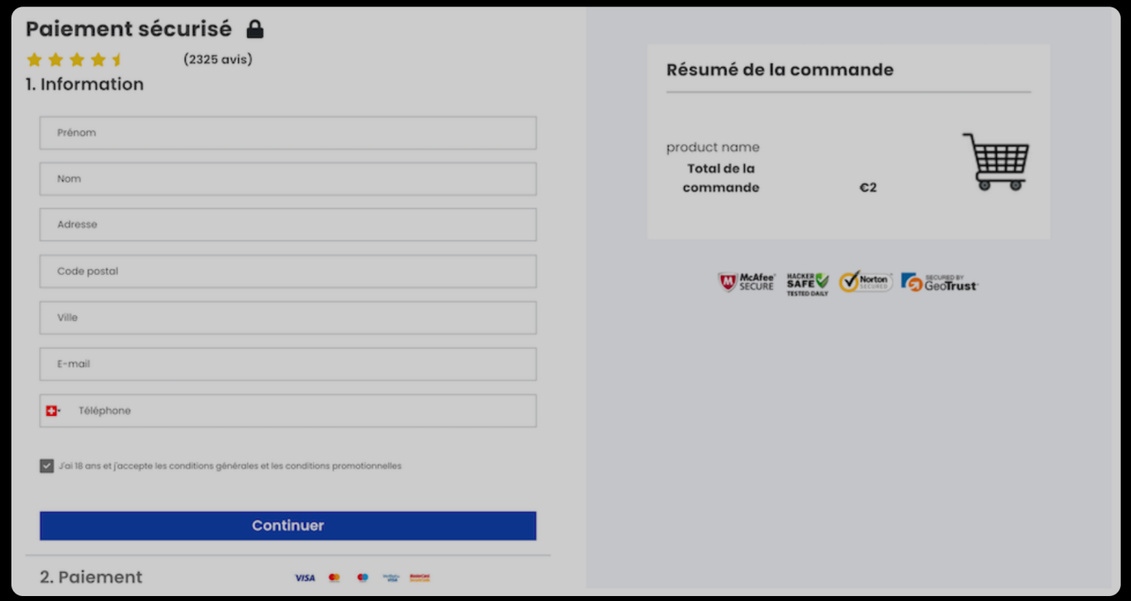


oops… VexTrio, you forgot a few…..

Blank Credit Card Submit “offers”

adtrafico.com/blog/

New Tier 2&3 Blank Page Offers

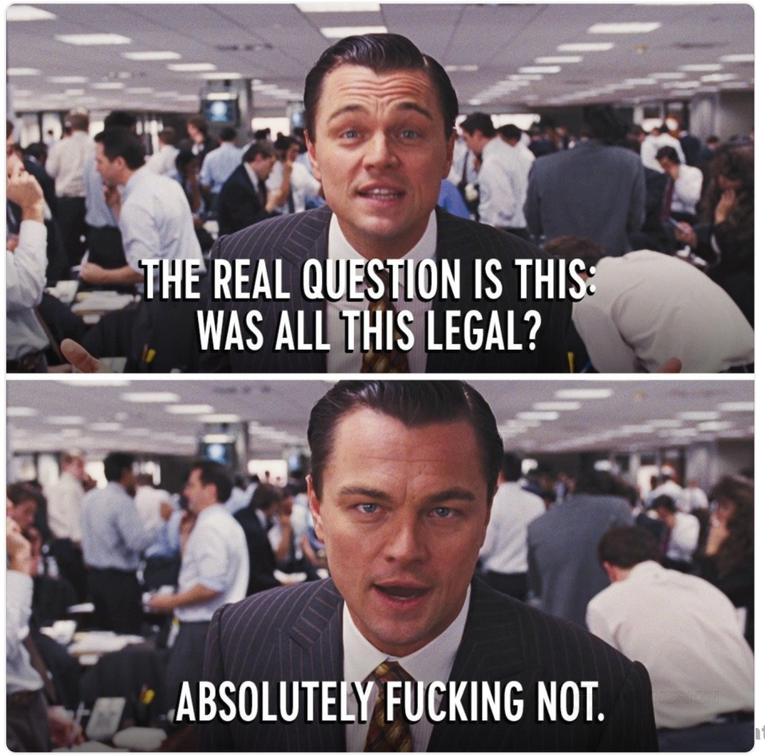


We've got some exciting news from Adtrafico. This week we've rolled out new Blank Pages specifically designed for Tier 2 and 3 countries. These offers are super customizable, with modifiable landing pages, pre-filled forms, and a Facebook pixel support via URL. Check out our latest Sweepstakes offer Dynamic Blank Express, available for a ton of GEOs.

Read more

New Offers 2024-10-25

adtraf:co



Fake Apps

play.google.com/store/apps/developer?id=CoreFlowz

Google Play Games Apps Movies & TV Books Kids

CoreFlowz

Spam Guard

Spam Guard - Spam Blocker
CoreFlowz
4.2 ★

MGuard

MGuard - Spam Protection
CoreFlowz
4.3 ★

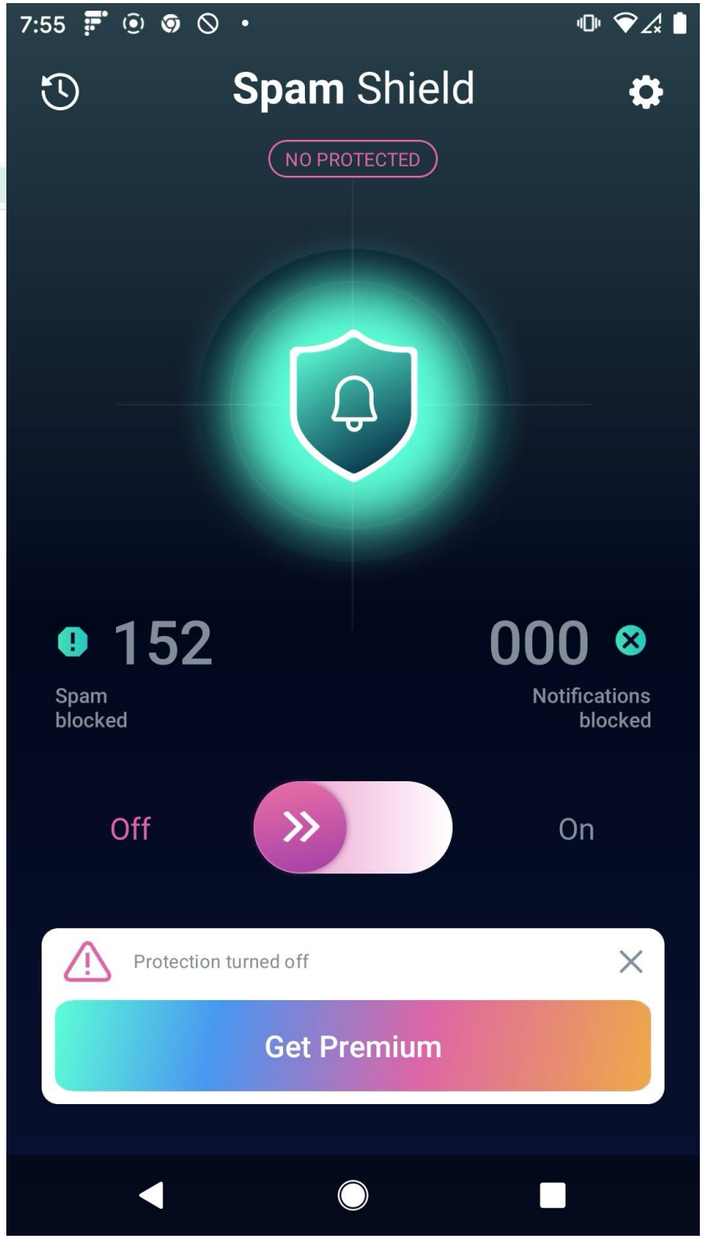
apps.apple.com/us/app/fast-vpn-with-ad-blocker/id1522664842

Store Mac iPad iPhone Watch

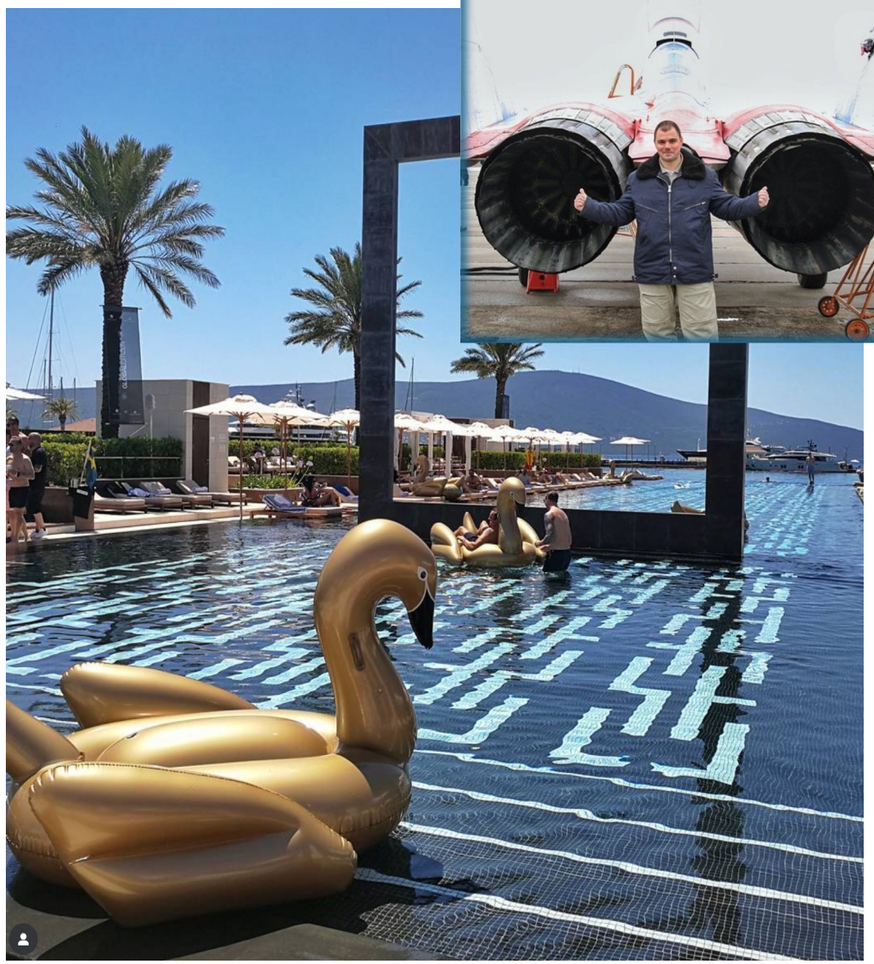
App Store Preview

This app i

Fast VPN with ad blocker 4+
Internet booster ad blocker
ALPHASCALE MEDIA GMBH
★★★★★ 4.3 • 162 Ratings
Free · Offers In-App Purchases



Scammers Take Vacations



Three Things

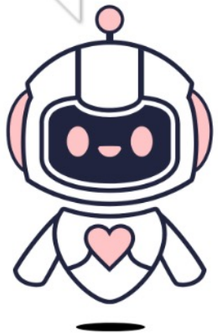
1. Malicious Adtech is a thing - we should all pay more attention!
2. The internet is an amazing place – make a backup!
3. Scamming is big business – private jets to Coldplay concerts!

….

Bonus: *If you have a globally unique name, change it before you go into crime.*

Read our research! Questions???

7B9605E6-87A9-4F28-A134-C2F1A15C1FDD



VexTrio
Fake
Captcha

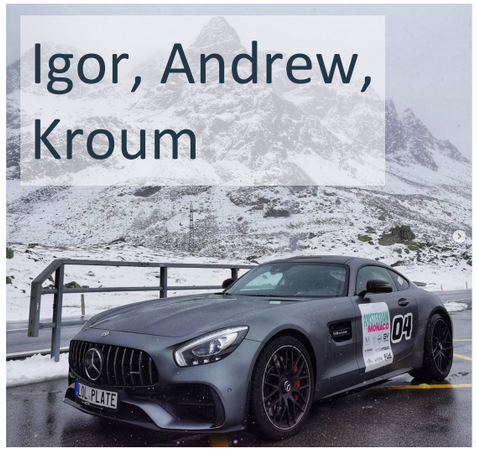
youtube.com/watch?v=f_jBRq7Gd_Y

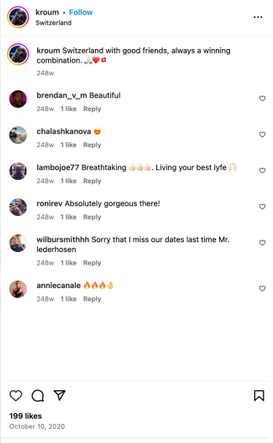
YouTube Search

Kroum Vassilev's Supersonic Flight to the Edge of Space

Kroum 21 subscribers Subscribe 4 Share Download Clip Save

210 views Apr 6, 2017





References

VexTrio's Relationship with Website Malware Actors

- Research released June 13, 2025 that reveals how VexTrio and several other TDS systems are related to each, driving large volumes of traffic from compromised websites for years. Deep dive into DNS TXT C2 and other adtech groups.

VexTrio at the Center of CyberCrime

- Research released January 2024 as an original expose of VexTrio's affiliate program and relationship with SocGholish, as well as other actors like ClearFake

VexTrio's Origin Story: From Spam to Scam to Adtech – release Aug 6th here.

VexTrio Unmasked: A Legacy of Spam and Home-Grown Scams – release ~Aug 12

Inside the Robot: Deconstructing VexTrio's Affiliate Advertising Network – release ~Aug 14