VALIDATION REPORT

CASE STUDY #004

Entity Category:

AI Platform Impersonation — One Day Old Domain

Submission Type:

Fake Creator Partnership Offer — Data Harvesting Infrastructure

This session was initiated upon receiving an unsolicited email claiming to represent the partnerships team of a well-known AI platform aggregator. The sending domain was registered one day before the email was sent. The website behind the domain displays branding entirely unrelated to the claimed platform. The site has zero public indexing. Entity names are withheld from public distribution.

DATE	ANALYST	SYSTEM	VERDICT
MAY 2026	VELURYN AGNECY	VASD v1.0	HIGH RISK — DATA HARVESTING

velurynandoc@gmail.com

SECTION 00

OPENING STATEMENT

Some scams are elaborate. Some are careless. This one is careless — and that carelessness is the most important finding in this session.

An entity claiming to represent the creator partnerships team of a major AI platform sent an outreach email from a domain registered the day before. Not a year before. Not a month before. One day. The domain was built, the email was written, and the outreach went out within a 24-hour window. That is not how a legitimate company operates. That is how a scam campaign launches.

The website behind the domain does not show the claimed platform. It shows a different brand entirely, with a form asking creators to submit their channel name, channel link, subscriber count, and email address. That form is not an application portal. It is a data collection mechanism.

> *"A domain registered yesterday is not an oversight. It is a construction date. The building was built for this email."*

— Core finding, Layer 1.

DOMAIN VERIFICATION

SUBMITTED DOMAIN VS REAL PLATFORM

FIELD	SUBMITTED DOMAIN	REAL PLATFORM DOMAIN	MATCH
Domain	poecontact.com	poe.com	NO
Registered	26 May 2026 — 1 day before email sent	Long-standing domain	NO
Registrant	GDPR masked — Finland	Quora, Inc. — USA	NO
Website Brand	JOIN.TEAM (unrelated branding)	Poe by Quora	NO
Google Index	Not indexed — zero public visibility	Fully indexed globally	NO

Five mismatches across five independent signals. Not one of them is explainable by administrative error or timing. The domain was built to impersonate. The website was built to collect. The email was built to deliver both to as many creators as possible.

SECTION 01

LAYER 1 — INITIAL SCREENING

Layer 1 does not need depth when the surface is this compromised. Every signal examined in the first pass returned a flag.

SIGNAL	FINDING	STATUS
Sending Domain	Email sent from hello@poecontact.com. The real platform operates exclusively from its primary registered domain. poecontact.com has no verified connection to the platform it claims to represent.	✕ HIGH RISK
Domain Age at Time of Email	poecontact.com was registered on 26 May 2026. The email was sent on 27 May 2026. The domain was one day old when this email was delivered. No legitimate company sends creator partnership outreach from a domain registered the previous day.	✕ HIGH RISK
Reply-To Address	Reply-to is set to hello@poecontact.com — the same unverified domain. Any reply from the creator goes directly to the scammer's infrastructure.	✕ HIGH RISK
Casual Tone as Disarming Device	The email opens with 'quick question' and uses informal language throughout. This is a deliberate friction-reduction technique. The lower the formality, the less scrutiny the recipient applies before replying.	■ FLAGGED
No Sender Title or Company Verification	The sender signs as 'Alex, Creator Partnerships, Poe Partners.' No LinkedIn, no company email signature, no verifiable employee record. The title is self-assigned and unverifiable.	■ FLAGGED

LAYER 01 VERDICT	INITIAL SCREENING
HIGH RISK — Domain one day old at time of sending. All contact infrastructure is unverified.	

The one day domain age is not a supporting flag. It is the primary finding. Everything else confirms it. But the domain age alone is sufficient to terminate engagement with this entity under any reasonable verification standard.

SECTION 02

LAYER 2 — REAL-WORLD PRESENCE

Layer 2 examined both the claimed platform and the actual domain. The gap between them is complete.

SIGNAL	FINDING	STATUS
Real Platform — Verified	The AI platform being impersonated is a legitimate, widely used product owned by a major technology company with a long-standing domain, global user base, and verified corporate identity.	✓ CLEAR
poecontact.com — No Connection to Real Platform	No affiliation, redirect, or reference connects poecontact.com to the real platform. The real platform's partnerships and creator programs operate through its primary domain only.	✕ HIGH RISK
Website Brand Mismatch	The website at poecontact.com displays the branding 'JOIN.TEAM' — entirely unrelated to the claimed platform. The visual identity, name, and positioning are completely different from the platform the email claims to represent.	✕ HIGH RISK
Google Index Status	poecontact.com has zero presence in Google search results. A platform claiming to manage creator partnerships for a major AI product has no public visibility of any kind.	✕ HIGH RISK
Registrant Identity	WHOIS data shows the registrant is located in Finland with all contact fields GDPR masked. No company name, no administrator name, no verifiable owner identity.	✕ HIGH RISK

LAYER 02 VERDICT	REAL-WORLD PRESENCE
HIGH RISK — Real platform confirmed. Sending domain confirmed as entirely unrelated. Website brand is a third, unrelated entity.	

SECTION 03

LAYER 3 — DEEP VERIFICATION

Layer 3 examines what the infrastructure was built to do. In this case, the website visible at poecontact.com reveals the objective directly.

SIGNAL	FINDING	STATUS
Data Harvesting Form	The website displays a form titled 'Apply now' requesting: channel name, channel link, subscriber count, and email address. This is not an application for a legitimate program. It is a structured data collection operation targeting content creators.	✕ HIGH RISK
Data Value to Attacker	Channel name and link provide a public profile. Subscriber count identifies high-value targets. Email address enables further targeted phishing. Together, this dataset is used to build a creator targeting list for future scam campaigns.	✕ HIGH RISK
Scam Infrastructure Timeline	Domain registered: 26 May 2026. Email sent: 27 May 2026. This timeline indicates a rapid-deployment scam operation — build the domain, launch the campaign, collect data, and move before detection occurs.	✕ HIGH RISK
Brand Layering	The email uses one brand name. The website uses a different brand name. This split is intentional — it creates confusion about which entity is responsible and makes reporting and tracking significantly harder.	✕ HIGH RISK
No Creator Protection Offered	The email mentions 'no scripts, no approval back-and-forth' as selling points. In a legitimate deal, these would be negotiated terms. Eliminating them in advance removes the protective friction that legitimate brands maintain.	■ FLAGGED

LAYER 03 VERDICT	DEEP VERIFICATION
HIGH RISK — Infrastructure confirmed as data harvesting operation. Two brand identities used across email and website to obscure origin.	

SECTION 04

FINAL JUDGMENT

VERDICT: HIGH RISK — DATA HARVESTING

This email does not represent the platform it names.

The domain it operates from was registered 24 hours before the email was sent. The website behind that domain carries a completely different brand name and displays a form designed to collect creator data — channel identity, audience size, and contact information.

The real platform is legitimate, widely used, and entirely uninvolved in this communication.

What this operation is: a rapid-deployment impersonation campaign targeting content creators. The email harvests trust using a recognized brand name. The website harvests data using a form that looks like an application portal. The data collected is used to identify and target high-value creators in future campaigns.

A creator who submits their details through the website linked in this email has provided a complete targeting profile to an anonymous entity in an unknown location operating behind a one-day-old domain.

RECOMMENDATION: Do not reply to this email. Do not visit the linked website. Do not submit any channel or contact information through any form connected to this outreach. If you want to explore a legitimate partnership with the real platform, visit their official website directly and contact their verified partnerships team.

LAYER SUMMARY

LAYER	NAME	FLAGS	RESULT
01	Initial Screening	5	HIGH RISK
02	Real-World Presence	4	HIGH RISK
03	Deep Verification	5	HIGH RISK

FINAL	**Combined Judgment**	**14**	**HIGH RISK — DATA HARVESTING**

FULL SERIES OVERVIEW

CASE	TITLE	THREAT TYPE	VERDICT
#001	Credibility Inflation	Unverified accreditations and inconsistent claims	SUSPICIOUS
#002	Labor Extraction	Affiliate recruitment disguised as partnership	HIGH RISK
#003	Malware Delivery	Windows-only contract link — confirmed malware pattern	HIGH RISK — MALWARE
#004	**Data Harvesting**	**One day old domain — creator data collection form**	**HIGH RISK — DATA HARVESTING**

This report was produced by VELURYN AGNECY — VASD Division. For inquiries: velurynandoc@gmail.com