THREAT INTELLIGENCE REPORT

MutaCryptor Scam Network

Crypto-Enabled Internship Fraud Campaign

Correlation Analysis: MutaEngine | VRV Security | Zorvyn FinTech

Report ID	CNTI-2026-001
Version	2.0 — Updated 18 April 2026
Author	Nathaniel T.O (Cyber Nate)
Organization	Cyber Nate Intelligence & Forensics
Classification	TLP: WHITE — Unrestricted Public Disclosure
Threat Actor	Unattributed | Suspected India-based Fraud Ring
Severity	**HIGH — Active, large-scale, global targeting**
Victim Profile	Cybersecurity / tech job seekers globally (India, Nigeria, others)
Key Finding	**Crypto-only (Bitcoin) payment system confirms deliberate untraceability**

1. Executive Summary

This report documents a coordinated internship fraud network actively targeting technology and cybersecurity job seekers globally since at least mid-2024. The operation creates elaborate fake companies with professional-grade websites, employee portals, legally styled offer letters, and automated onboarding infrastructure, then exploits the trust built over an extended fake onboarding period to solicit cryptocurrency payments for a software product called **MutaCryptor**, developed by an entity called **MutaEngine**.

Two confirmed fake company shells have been identified — **VRV Security** and **Zorvyn FinTech** — with evidence suggesting additional shells may be in operation simultaneously. The author of this report was personally targeted by the **Zorvyn FinTech** operation in **April 2026**, enabling firsthand documentation of the complete attack chain from initial contact through the monetization phase and subsequent infrastructure collapse.

Critical new findings in this version of the report confirm that **MutaEngine** accepts payment exclusively via Bitcoin using dynamically rotating wallet addresses with 15-minute invoice expiration — a design that is inherently untraceable and irreversible, inconsistent with any legitimate software vendor, and strongly indicative of deliberate criminal financial architecture. The operation's infrastructure subsequently collapsed (NXDOMAIN) during the investigation, consistent with a campaign teardown following exposure.

2. Background & Context

2.1 Discovery

On 7 April 2026, the author received a screening assessment invitation from hr@zorvyn.io for a Cybersecurity Analyst Intern position at Zorvyn FinTech Pvt. Ltd. After completing a timed technical assessment, an offer letter dated 3 April 2026 was issued, signed by a purported CEO Raj Kishor Pattnaik, offering a monthly stipend of INR 45,000 with a Pre-Placement Offer opportunity of up to INR 16 LPA.

Over the following days an extensive onboarding process unfolded including employee portal access, a welcome kit order (including a Dell Pro 14 laptop, branded merchandise, and accessories), and a welcome message from a reporting manager named Mudiwa Mkonto. On 13 April 2026 — the stated start date — Mudiwa Mkonto sent a training task email directing the author to purchase MutaCryptor software from mutaengine.cloud, with a reimbursement promise upon invoice submission. No purchase was made. This report documents the investigation that followed.

2.2 Prior Reports

The VRV Security variant of this scam was publicly reported on Glassdoor in February 2025, with additional exposure by researcher Rishi Raam on X (formerly Twitter) in December 2024. The Zorvyn FinTech variant received significant public attention in April 2026 across Reddit, Grapevine, and Indian tech forums. The author's investigation constitutes the first structured, evidence-based threat intelligence report correlating all three entities — MutaEngine, VRV Security, and Zorvyn FinTech — into a single network analysis.

3. Threat Actor Profile

Designation	Unattributed | Internal Tracking: INTERN-FRAUD-01
Active Since	August 2024 (MutaEngine domain first analyzed). VRV Security variant active by November 2024
Geography	Suspected Ghaziabad/NCR India-based operation. Victims confirmed globally including India and Nigeria
Motivation	Financial: direct Bitcoin revenue from software sales + PII/data harvesting for secondary monetization
Sophistication	**HIGH — Custom web infrastructure, AI-generated personas, stolen identities, automated onboarding, crypto obfuscation**
MutaEngine Founder	Bharti Kumari Singh, Ghaziabad, India (identified via Wellfound profile)
MutaEngine Funding	$10,000 seed (February 2024) — suspiciously small for claimed enterprise-scale product
Scale	Hundreds of victims confirmed across Glassdoor, Reddit, X, Grapevine, and international forums
Payment Model	**Bitcoin-only, rotating wallet addresses, 15-min invoice expiry — deliberately untraceable**

4. Infrastructure Analysis

4.1 Zorvyn FinTech

Zorvyn FinTech Pvt. Ltd. presents as a Bengaluru-based fintech company. Independent investigation confirms no verifiable corporate registration exists under Indian company law. The domain zorvyn.io scored 30.7/100 on Scam Detector, flagged for suspected phishing and spam activity. Employee profile photos on LinkedIn exhibited characteristics consistent with AI-generated synthetic identities.

Primary domain	zorvyn.io (Hostinger, low-cost shared hosting)
Employee portal	workplace.zorvyn.live — full-featured fake HR platform
Other subdomains	screening.zorvyn.live | employeesupport.zorvyn.live | onboarding@zorvyn.live
Email domains	hr@zorvyn.io | onboarding@zorvyn.io | logistics@zorvyn.live | mudiwamkonto@zorvyn.live
Status (Apr 18)	**COLLAPSED — NXDOMAIN returned for all zorvyn.live infrastructure**

4.2 VRV Security

VRV Security (vrvsecurity.in) operated as a prior shell company in this network. ScamAdviser assigned it a trust score of 2/100. The real VRV Security Cum Manpower Agency, a legitimate Indian security staffing firm, published a public notice confirming their identity had been stolen. An independent

investigation by researcher **Rishi Raam** confirmed the address on the fraudulent offer letters resolved to the real manpower agency's location, and the director's real name (**Vinod Kumar**) was replicated in the scam persona.

4.3 MutaEngine / MutaCryptor

MutaEngine (mutaengine.cloud) is the software vendor whose product MutaCryptor is the consistent and exclusive monetization instrument across all identified fake company shells. MutaEngine is registered on Internshala (hiring since 2024, 0 candidates hired) and Wellfound. The identified founder is Bharti Kumari Singh, Ghaziabad, India.

4.4 Cryptocurrency Payment Infrastructure (Critical Finding)

MutaEngine accepts payment exclusively via Bitcoin — no card, no PayPal, no regulated payment processor of any kind. This finding constitutes the single most significant indicator of criminal intent in this investigation. Legitimate software companies do not exclusively accept cryptocurrency. The implementation details confirm a sophisticated automated payment system designed for maximum untraceability:

- Bitcoin-only checkout — no alternative payment method available
- Dynamically rotating wallet addresses — each transaction receives a unique wallet address
- 15-minute invoice expiration — creates urgency and limits the window for blockchain analysis
- No KYC/identity verification required from buyer
- No refund or chargeback mechanism — all transfers are irreversible
- Payment portal hosted at pay.mutaengine.cloud — a separate subdomain from the main site
- Third wallet address also identified: bc1qvgka8h7z2wzu7jzqcspvlp9fcte6y6spvul84a
- Global pricing in USD ($34.99/year Pro, $29.99/year Lite) confirming international victim targeting

The use of dynamically generated Bitcoin wallet addresses with short-lived invoices strongly indicates automated cryptocurrency payment processing infrastructure designed to obfuscate fund tracing and enable scalable fraud operations. Funds received are presumed to pass through aggregation/mixing services before reaching a threat actor controlled master wallet, making chain-of-custody tracing extremely challenging without specialist blockchain forensics tools.

Evidence — Bitcoin Payment Interface (First observation, ~$34.99):

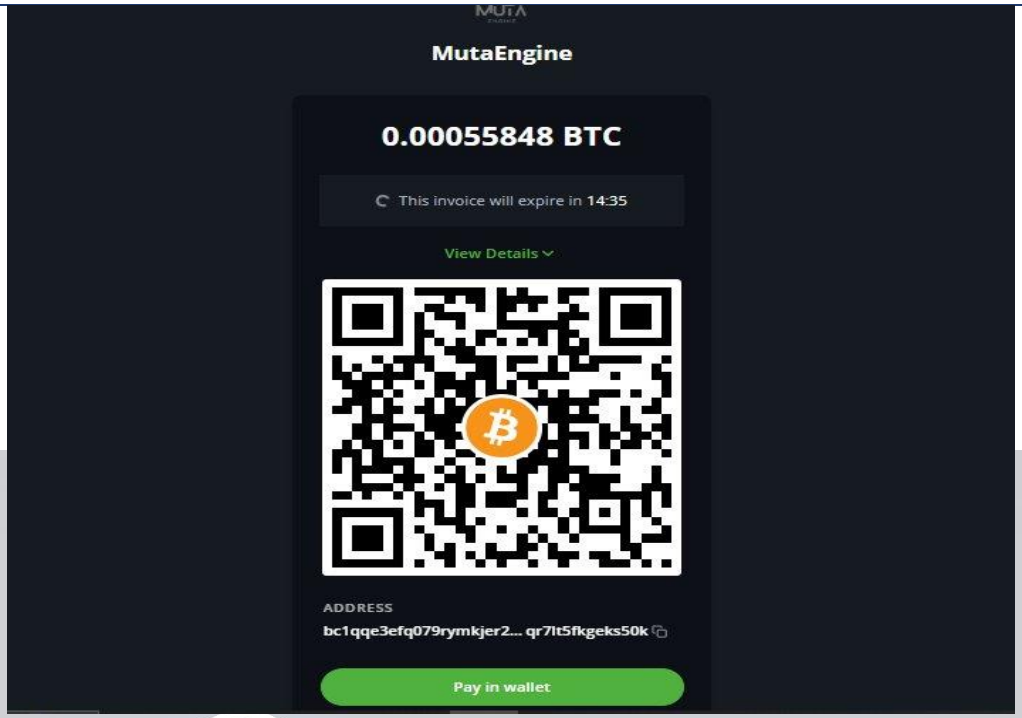

Figure 3a: MutaCryptor Pro Bitcoin-only checkout showing 0.00055848 BTC (~$34.99), 14:35 expiry, and wallet address bc1qqe3efq079rymkjer2...qr7lt5fkgeks50k

Evidence — Bitcoin Payment Interface (Second observation, different wallet — confirms rotation):

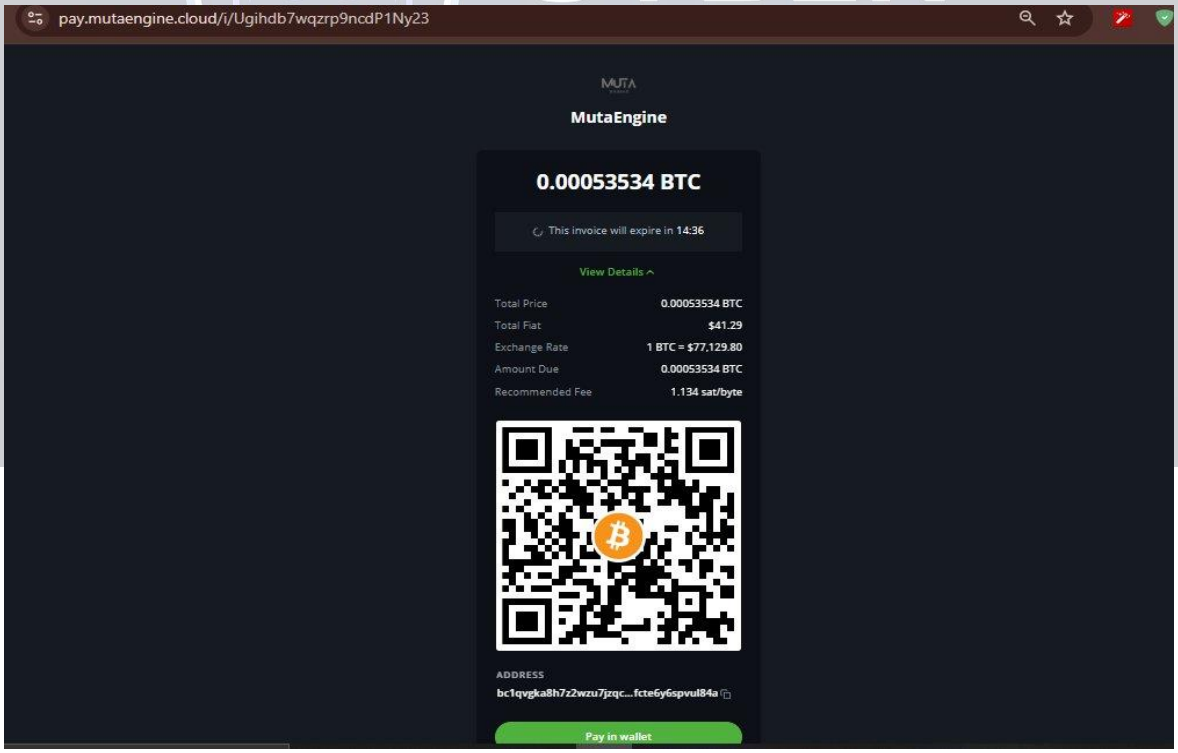

Figure 3b: Second MutaCryptor Pro checkout showing 0.00053534 BTC ($41.29 at different BTC rate), new wallet bc1qvgka8h7z2wzu7jzqc...fcte6y6spvul84a — wallet rotation confirmed

Evidence — MutaCryptor Pro pricing page ($34.99/year):

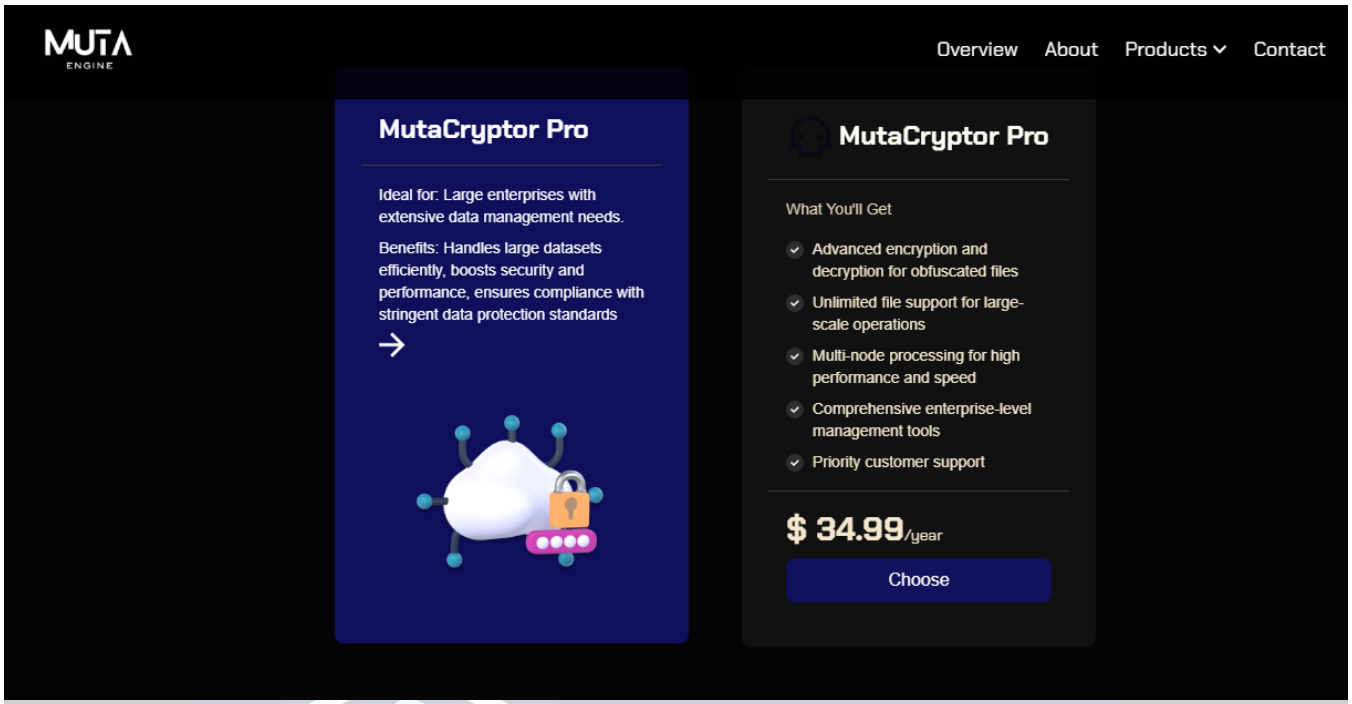

Figure 3c: MutaCryptor Pro product page showing $34.99/year pricing and enterprise feature claims

4.5 Infrastructure Collapse (NXDOMAIN — 18 April 2026)

During the course of the investigation, the domain zorvyn.live became entirely unreachable, returning NXDOMAIN responses for both web and MX (mail exchange) queries. The employee portal (workplace.zorvyn.live/profile) returned DNS_PROBE_FINISHED_NXDOMAIN. Email sent to mudiwamkonto@zorvyn.live bounced with the error: DNS type 'mx' lookup of zorvyn.live responded with code NXDOMAIN — domain name not found.

This infrastructure collapse is consistent with fraudulent campaigns deliberately tearing down after exposure, cycling to a new domain/shell company identity while retaining the underlying payment infrastructure. It also confirms the operation is not a legitimate company — no real business terminates its email infrastructure without notice.

Evidence — DNS bounce / NXDOMAIN (email delivery failure):

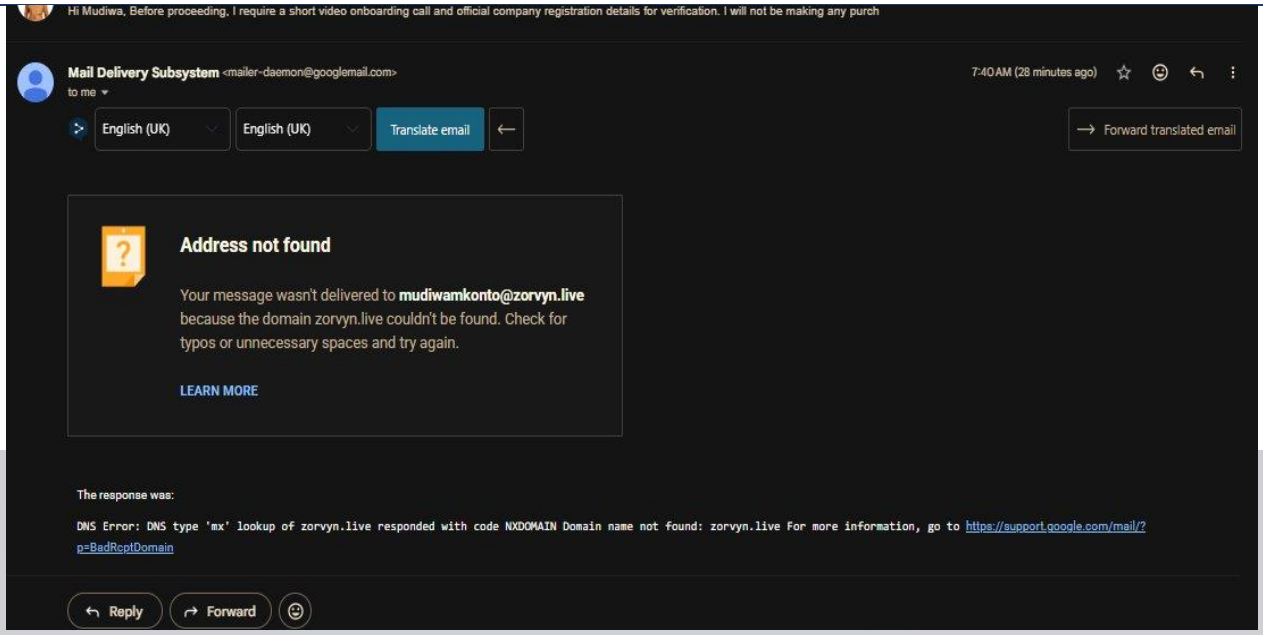

Figure 4a: Gmail Mail Delivery Subsystem error — mudiwamkonto@zorvyn.live — NXDOMAIN (18 April 2026)

Evidence — Employee portal unreachable:

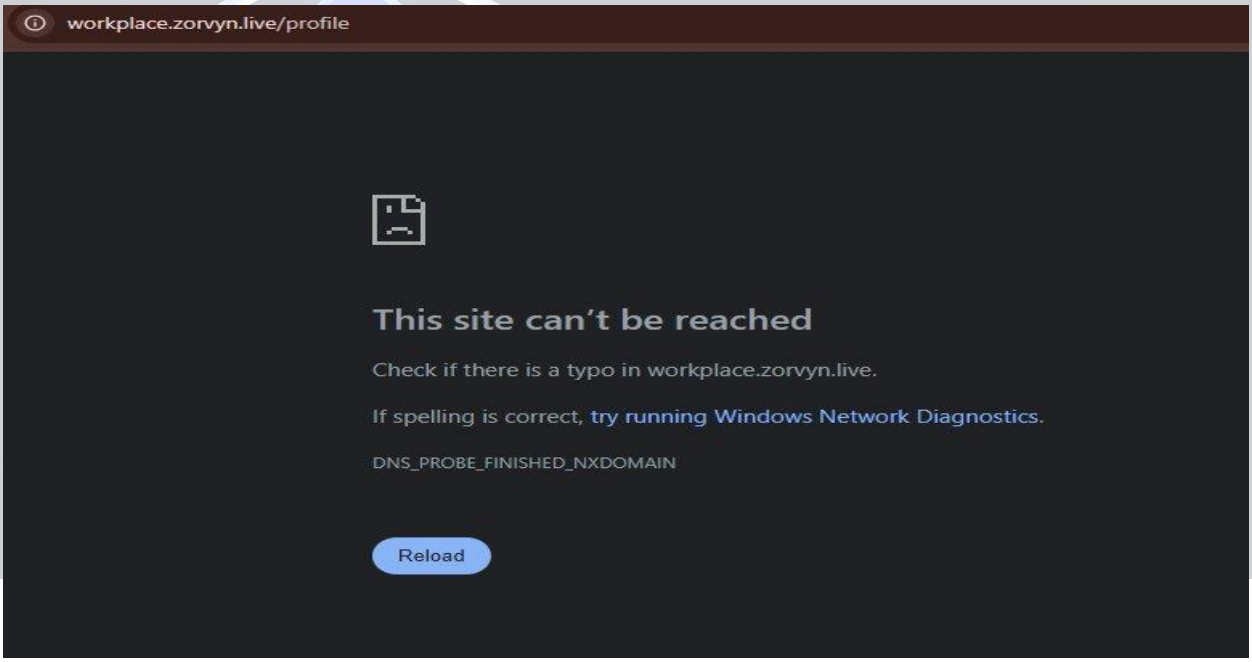

Figure 4b: workplace.zorvyn.live returning DNS_PROBE_FINISHED_NXDOMAIN — full infrastructure collapse confirmed

5. Attack Chain Analysis

The attack follows an 8-phase social engineering lifecycle consistent with a long-con trust-building strategy. Each phase deepens victim commitment before the monetization request is made. The chain was personally documented by the author across the full Zorvyn campaign.

Evidence — Full Zorvyn email campaign (inbox view showing complete automated sequence):

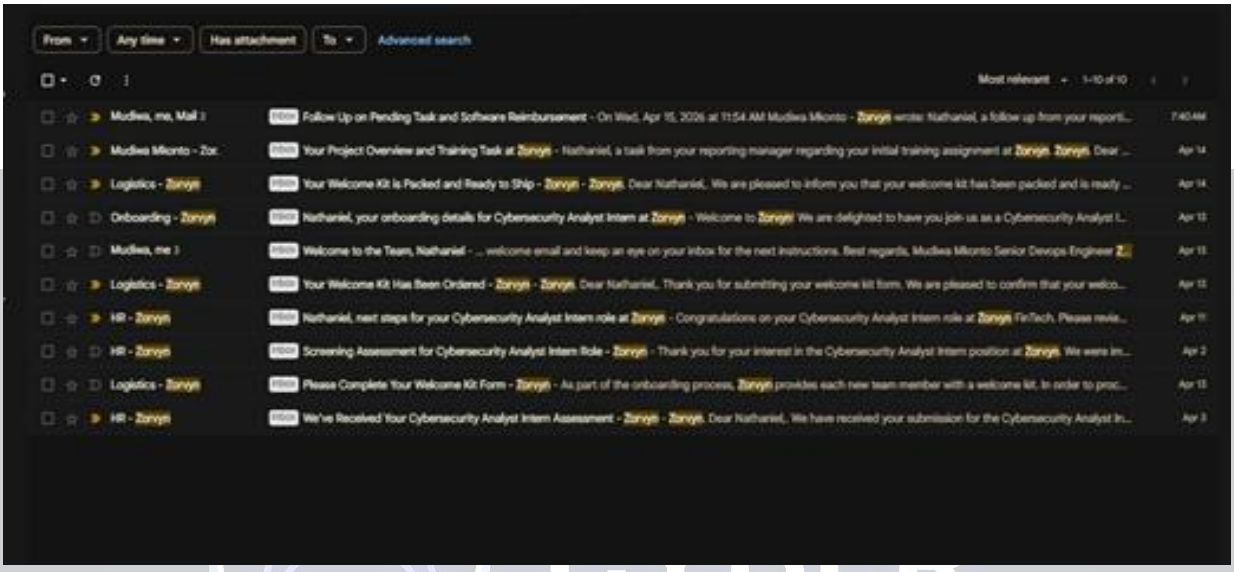

Figure 5a: Complete Zorvyn email sequence — 10 emails across 13–18 April 2026, including screening, offer, onboarding, logistics, training task, follow-up, and bounce

Figure 1 — End-to-End Social Engineering and Monetization Workflow:

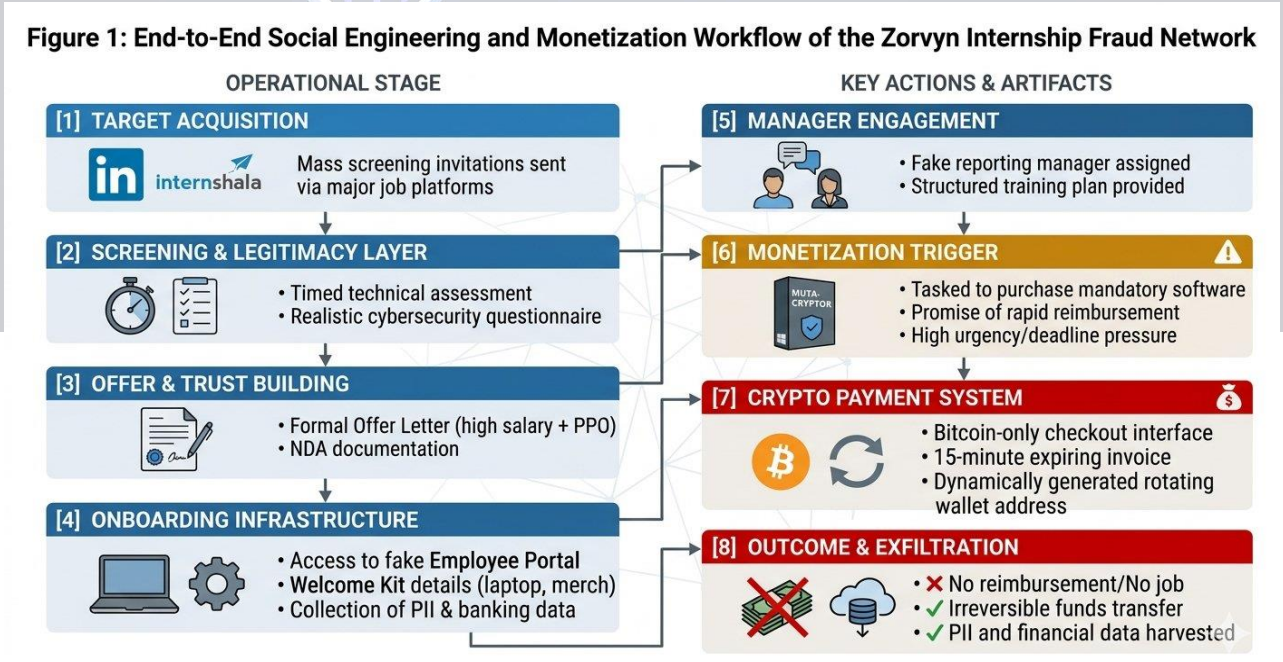

Figure 1: End-to-End Social Engineering and Monetization Workflow of the Zorvyn Internship Fraud Network (Nathaniel T.O, April 2026)

Phase 1 — Target Acquisition

- Victim profiles sourced from Internshala, LinkedIn, and other job platforms
- Mass screening assessment invitations sent to hundreds of candidates simultaneously
- Assessment designed to appear legitimate — timed, realistic technical cybersecurity questions
- Broad targeting: cybersecurity, software dev, data analysis, finance roles

Phase 2 — Screening & Legitimacy Layer

- Timed 90-minute multiple-choice assessment on real cybersecurity topics
- Assessment delivery via professional branded portal (screening.zorvyn.live)
- Designed to make candidates feel they earned selection — increasing psychological investment

Phase 3 — Offer & Trust Building

- Formal offer letter with NDA, leave policy, code of conduct, and CEO signature
- Stipend set above market rate (INR 45,000/month) to maximize acceptance rate
- PPO dangled (up to INR 16–18 LPA) to deepen long-term investment
- Explicit statement: 'Zorvyn never charges fees' — designed to lower security guard

Phase 4 — Onboarding Infrastructure Engagement

- Employee portal access — Dashboard, Payroll, Logistics, Documents, Webmail, Referrals
- Welcome kit order with premium items (Dell Pro 14, backpack, merch) to build credibility
- PII harvested: full name, home address, passport photo, ID card photo
- Payment/banking details collected under cover of payroll setup

Evidence — Onboarding email (portal credentials):

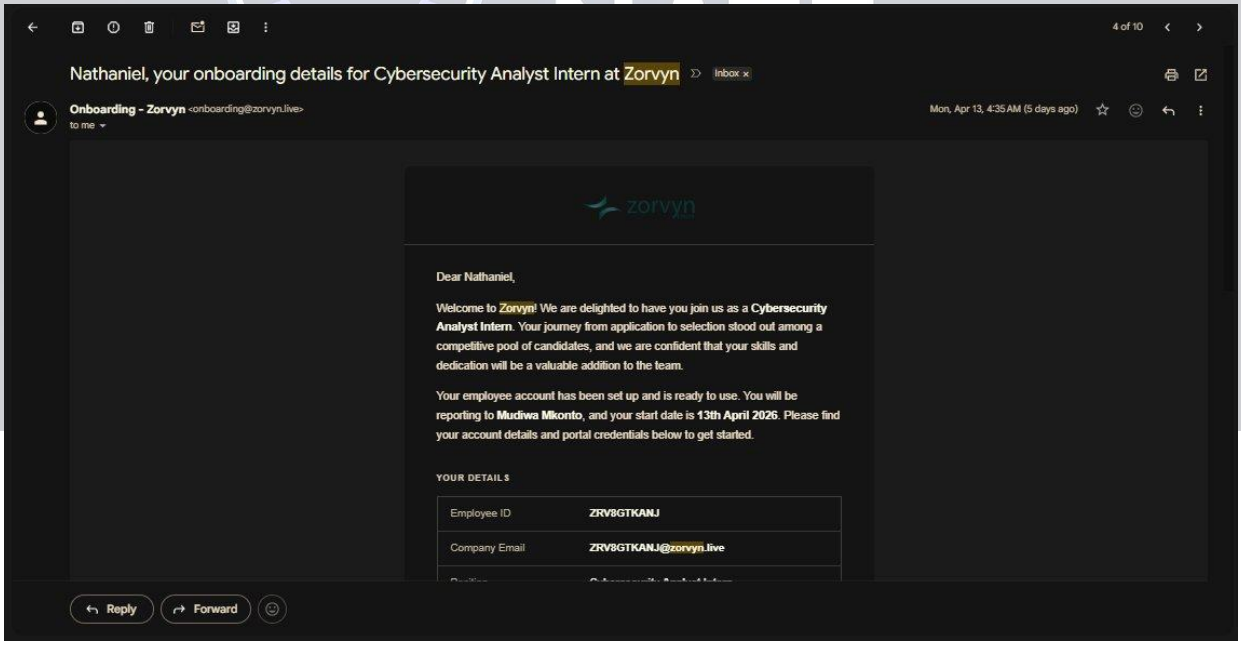

Figure 5b: Onboarding email from onboarding@zorvyn.live — employee ID ZRV8GTKANJ, company email ZRV8GTKANJ@zorvyn.live assigned

Evidence — Welcome kit ordered confirmation:

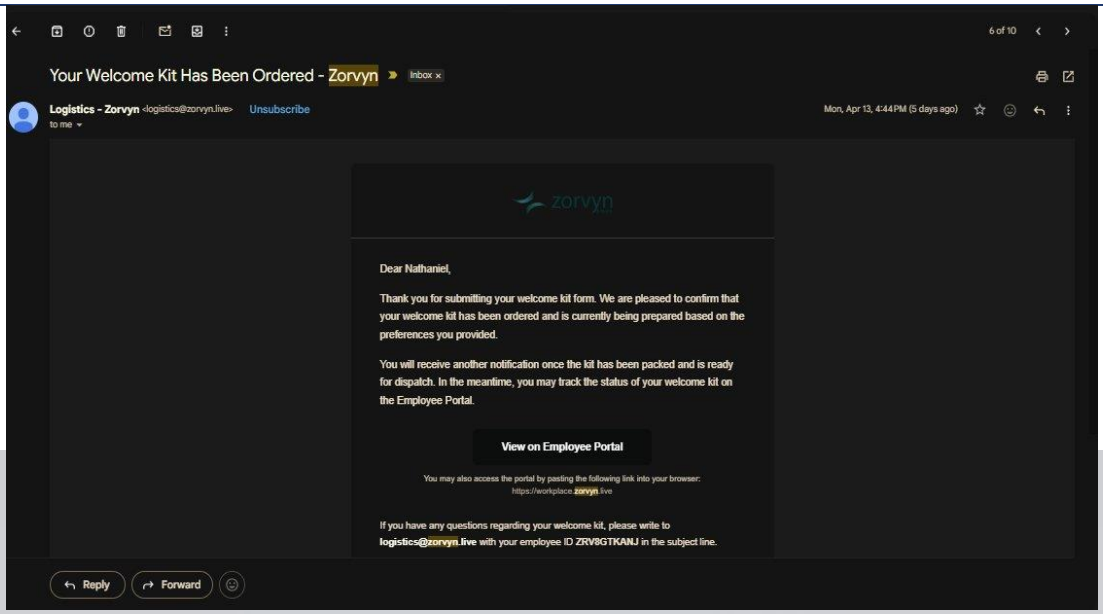

Figure 5c: Logistics email confirming welcome kit order — automated trigger after form submission

Phase 5 — Manager Introduction & Training Framing

- Fake reporting manager Mudiwa Mkonto contacts victim with warm welcome email
- Detailed 15-day training plan issued covering real cybersecurity domains — adds technical credibility
- Company context established around fintech security and obfuscation tools — primes the purchase ask
- Manager uses zorvyn.live domain — separate from zorvyn.io — to appear as internal employee system

Evidence — Offer letter email (official offer with Mudiwa Mkonto as reporting manager):

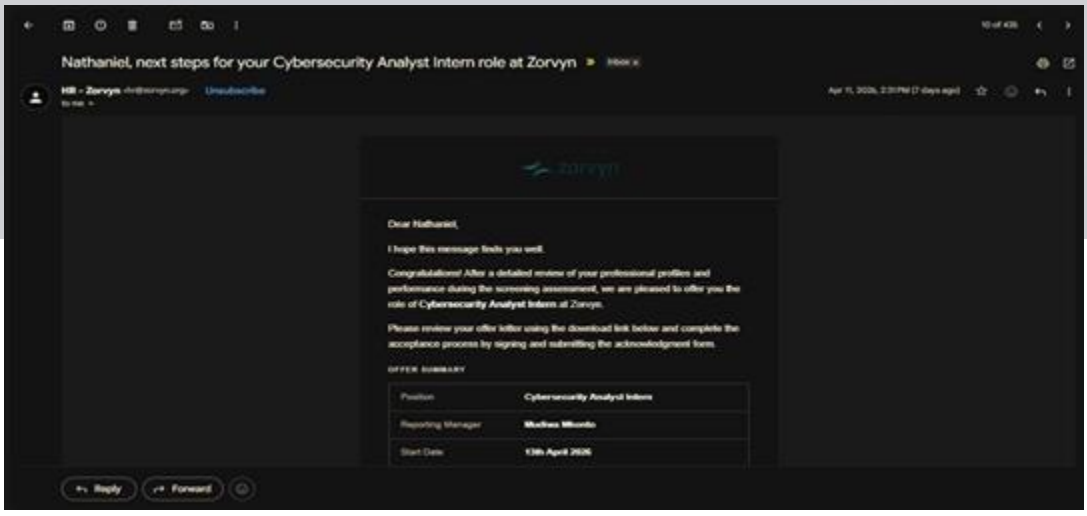

Figure 5d: HR email from hr@zorvyn.org confirming Cybersecurity Analyst Intern offer — reporting manager Mudiwa Mkonto, start date 13 April 2026

Phase 6 — Monetization Trigger

- Training task email singles out reverse engineering and obfuscation as focus area — directly primes MutaCryptor
- Victim instructed to purchase MutaCryptor Lite and/or Pro from mutaengine.cloud
- Urgency applied: 48-hour submission deadline on task and software reimbursement
- Pre-filled reimbursement form at employeesupport.zorvyn.live to simulate legitimate process
- Explicit confidentiality clause: 'Do not discuss details with anyone' — isolation tactic
- 'Do not use AI tools' instruction — designed to prevent research that would expose the scam
- Follow-up pressure email sent April 15 warning that non-purchase blocks project team access

Evidence — Follow-up pressure email warning from Mudiwa Mkonto

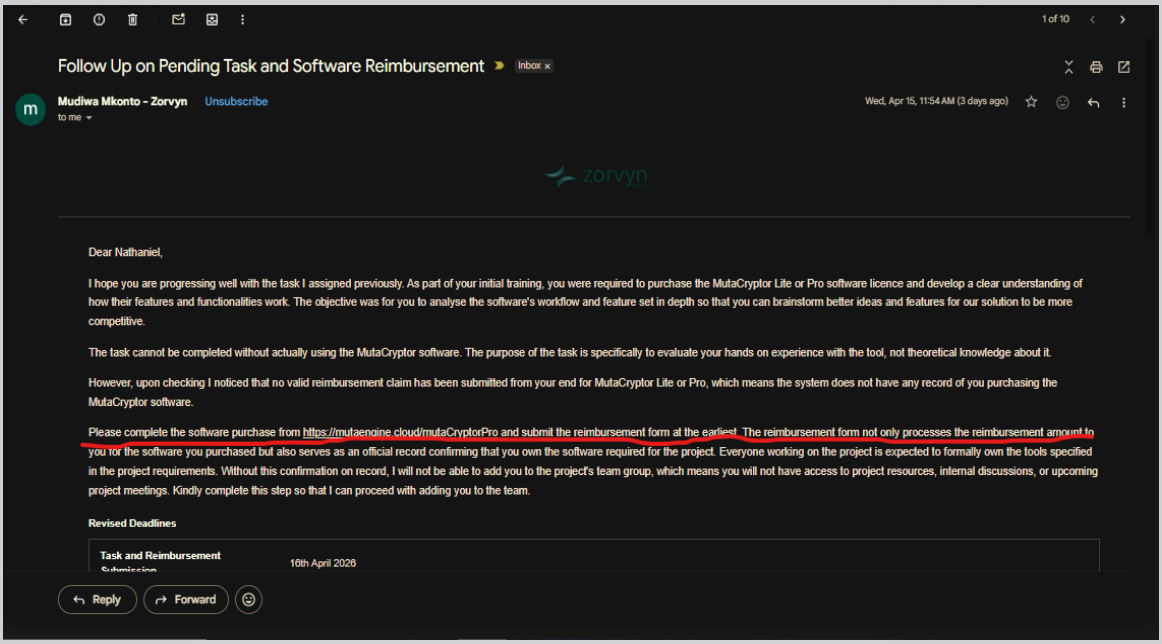

Figure 5e: Follow-up pressure email sent April 15 from Mudiwa Mkonto (Reporting Manager) warning that non-purchase blocks project team access

Phase 7 — Crypto Payment Extraction

- Bitcoin-only checkout at pay.mutaengine.cloud — no card or traditional payment option
- Dynamic wallet address generated per transaction — prevents direct cross-victim wallet linking
- 15-minute invoice expiry — urgency pressure to pay before research is conducted
- Funds transferred are irreversible — no chargeback, no refund mechanism
- Funds presumed routed through aggregation/mixing to threat actor master wallet

Phase 8 — Data Retention & Infrastructure Teardown

- PII already collected regardless of whether purchase occurs — name, photo, address, payment details
- Data harvestable for identity fraud, dark web sale, or future targeted attacks
- Infrastructure torn down (NXDOMAIN) after exposure — cycle restarts under new shell company identity
- No reimbursement issued, no job exists, no welcome kit shipped

6. Cryptocurrency Payment Obfuscation Mechanism

The cryptocurrency payment architecture used by MutaEngine represents a deliberate and sophisticated approach to financial obfuscation. The mechanism is structured across two layers — a visible transaction layer presented to the victim, and a backend obfuscation layer that prevents fund tracing.

Figure 2: Cryptocurrency Payment Obfuscation Mechanism Using Dynamic Wallet Generation

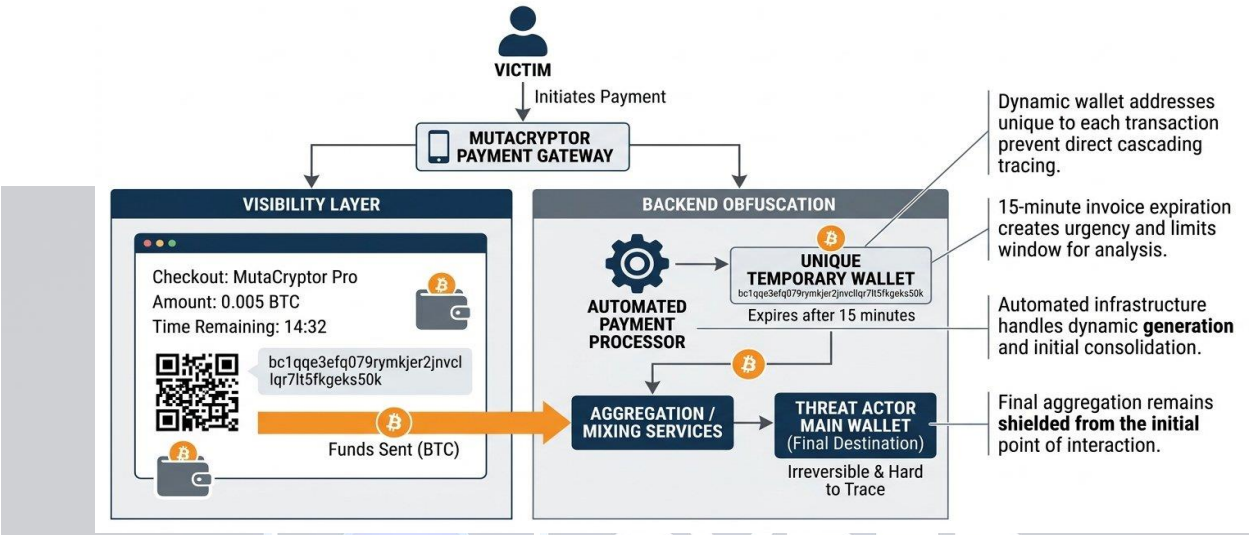

Figure 2: Cryptocurrency Payment Obfuscation Mechanism Using Dynamic Wallet Generation (Nathaniel T.O, April 2026)

6.1 Visible Layer

The victim sees a professional-looking Bitcoin checkout interface at pay.mutaengine.cloud/i/[unique_ID]. The page displays the MutaEngine branding, the BTC amount equivalent to the product price, a countdown timer, a QR code, and a unique wallet address. This interface appears to be powered by a self-hosted or third-party crypto payment processor.

6.2 Backend Obfuscation Layer

Each victim receives a dynamically generated temporary wallet address unique to their transaction. This prevents investigators from linking multiple victims to a single wallet through blockchain analysis. Once the invoice expires after 15 minutes, the temporary wallet is abandoned regardless of whether funds were received, and a new one is generated for the next victim. Received funds are presumed to be aggregated and routed through mixing/tumbling services before reaching a threat actor-controlled master wallet that remains shielded from any initial point of victim interaction.

6.3 Confirmed Wallet Addresses

Wallet ID	Address	Observed
Wallet 1	bc1qqe3efq079rymkjer2jnvcllqr7lt5fkgeks50k	~14 Apr 2026
Wallet 2	bc1q2h0q5z4lkd9zvaq3twp4cv3gpa0xj5elqem7s7	~15 Apr 2026
Wallet 3	bc1qvgka8h7z2wzu7jzqcspvlp9fcte6y6spvul84a	~16 Apr 2026

All three wallets confirmed as unique per-transaction temporary addresses. Rotation confirmed within 48 hours — strongly indicating automated wallet generation infrastructure rather than manual assignment.

7. Tactics, Techniques & Procedures (TTPs)

Mapped to MITRE ATT&CK where applicable. Note: this is a criminal fraud network; several techniques are adapted from enterprise threat frameworks to the social engineering and financial fraud context.

Tactic	Technique	Description
Initial Access	Phishing (T1566)	Mass distribution of fake job screening invitations via legitimate email infrastructure
Resource Development	Establish Infrastructure (T1583)	Custom domains, employee portals, email systems, and payment gateways created
Resource Development	Compromise Infrastructure (T1584)	Real company identity (VRV Security, Vinod Kumar) stolen and impersonated
Resource Development	Develop Capabilities (T1587)	AI-generated synthetic employee personas deployed on LinkedIn and company portals
Collection	Data from Info Repositories	Personal data, photos, addresses, and payment info harvested via onboarding forms
Social Engineering	Trust Building — Extended	Multi-week onboarding with premium welcome kit, salary, and manager contact deepens commitment
Social Engineering	Urgency + Isolation	48-hour deadline and confidentiality clause prevent victim from seeking external advice
Exfiltration	Exfiltration Over Web (T1567)	Victim PII/data submitted to attacker-controlled portals and forms
Impact	Financial Theft — Crypto	Victims directed to Bitcoin-only checkout; funds are irreversible and untraceable
Defense Evasion	Infrastructure Teardown	Domain and email infrastructure abandoned (NXDOMAIN) after exposure detection
Impact	Automation at Scale	Dynamic wallet generation, templated onboarding flows, triggered email sequences confirm automated fraud platform

8. Indicators of Compromise (IOCs)

IOC Type	Value	Confidence
Domain	zorvyn.io — primary public domain (Hostinger)	**High**
Domain	zorvyn.live — internal employee domain (NXDOMAIN)	**High**
Domain	workplace.zorvyn.live — employee portal (NXDOMAIN)	**High**
Domain	screening.zorvyn.live — assessment platform	**High**
Domain	employeesupport.zorvyn.live — reimbursement forms	**High**
Domain	pay.mutaengine.cloud — Bitcoin payment gateway	**High**
Domain	mutaengine.cloud — MutaCryptor vendor site	**High**

Domain	vrvsecurity.in — prior shell company (trust score 2/100)	**High**
Email	hr@zorvyn.io | hr@zorvyn.org	**High**
Email	onboarding@zorvyn.io | onboarding@zorvyn.live	**High**
Email	logistics@zorvyn.live	**High**
Email	mudiwamkonto@zorvyn.live (fake manager)	**High**
Email	ceo@mutaengine.cloud	**Medium**
Software	MutaCryptor Lite / MutaCryptor Pro — payment trigger	**High**
BTC Wallet	bc1qqe3efq079rymkjer2jnvcllqr7lt5fkgeks50k	**High**
BTC Wallet	bc1q2h0q5z4lkd9zvaq3twp4cv3gpa0xj5elqem7s7	**High**
BTC Wallet	bc1qvgka8h7z2wzu7jzqcspvlp9fcte6y6spvul84a	**High**
Crypto Pattern	Rotating BTC wallets with 15-min expiry invoices	**High**
Payment URL	pay.mutaengine.cloud/i/[unique_invoice_ID]	**High**
Person	Raj Kishor Pattnaik — fake CEO persona on offer letter	**High**
Person	Mudiwa Mkonto — fake Sr. DevOps Engineer / reporting manager	**High**
Person	Bharti Kumari Singh — identified MutaEngine founder (Ghaziabad)	**Medium**
Employee ID	ZRV8GTKANJ (author's assigned employee ID)	**Medium**
Infrastructure	Hostinger hosting — low-cost provider with phishing host history	**Medium**

9. Correlation Analysis: MutaEngine, VRV Security & Zorvyn

The central analytical question is whether MutaEngine operates independently of the fake company shells, or whether all three entities are controlled by the same threat actor. Three hypotheses are assessed. New evidence from the Bitcoin-only payment infrastructure significantly strengthens Hypothesis A.

Hypothesis A — Single Operator (Most Likely — Strengthened)

MutaEngine is owned and operated by the same threat actor who created VRV Security and Zorvyn FinTech. The fake companies serve purely as acquisition funnels directing victims to purchase a product from an entity that appears independent. The Bitcoin-only payment design creates plausible deniability — MutaEngine can claim it has no knowledge of how its software is marketed.

- Exclusive and consistent use of only MutaCryptor across all fake companies with zero variation
- Unified Bitcoin payment infrastructure at pay.mutaengine.cloud used across all campaigns
- MutaEngine itself posts hiring listings on Internshala — potentially feeding its own victim pipeline
- Domain privacy protection conceals MutaEngine owner identity
- VRV Security (late 2024) → Zorvyn FinTech (2025-2026) — iterative rebranding as each shell is exposed
- $10,000 seed funding is implausibly small for a genuine enterprise security product company
- 0 candidates hired across 2 Internshala postings — consistent with fake operation
- Infrastructure teardown (NXDOMAIN) upon exposure — consistent with campaign cycling behaviour

Hypothesis B — Affiliate Fraud (Possible)

MutaEngine runs an affiliate program. The threat actors signed up as affiliates and drive fraudulent purchases through fake companies. MutaEngine may be willfully blind to anomalous sales patterns.

- MutaEngine trust score (76) is higher than the shells — suggests some separation
- The Bitcoin-only payment model would still benefit MutaEngine regardless of affiliate structure
- Assessment: plausible but does not absolve MutaEngine of due diligence responsibility

Hypothesis C — Independent Exploitation (Least Likely)

The threat actors direct victims to purchase a legitimate third-party product without any financial relationship with MutaEngine. Assessment: no direct financial return model — dismissed as primary hypothesis. However, data harvesting from victims who visit the checkout page remains a secondary consideration.

10. Victim Impact Assessment

10.1 Financial

- MutaCryptor Lite: ~$29.99/year | MutaCryptor Pro: ~$34.99/year (USD, Bitcoin-only)
- All payments irreversible — no chargeback or refund possible via cryptocurrency
- With hundreds of simultaneous victims: estimated revenue per campaign cycle $15,000–$200,000+
- All revenue received in untraceable Bitcoin — no regulatory oversight or frozen funds possibility

10.2 Personal Data Exposure

- Physical home address — submitted via welcome kit form
- Passport-sized photograph — collected for fake ID card
- Banking / payment platform details — submitted to fake payroll portal
- Full legal name, email address, phone number — all submitted across onboarding forms
- Note: Author used a FGLEA Command address and newly created empty Payoneer account — minimising personal exposure

10.3 Psychological & Professional

- Extended trust betrayal across 1–2 weeks of detailed onboarding causes significant emotional distress
- Time investment in assessment, document submission, and onboarding cannot be recovered
- Reduced trust in legitimate remote employment opportunities — long-term career impact
- Victims who disclosed the 'internship' on CVs or LinkedIn may face reputational risk

10.4 Cryptocurrency Abuse Classification

- This operation constitutes cryptocurrency fraud — Bitcoin used as a deliberate financial evasion mechanism
- Rotating wallet addresses prevent standard blockchain tracing by victims or basic law enforcement
- 15-minute invoice expiration further reduces analysis window for any individual transaction
- Mixing/tumbling services presumed to be used to launder aggregated proceeds
- Classification: Cryptocurrency-enabled fraud / financial crime — reportable to EFCC, CBI, Interpol

11. Recommendations

For Job Seekers

- Verify company registration against official government registries before accepting any offer
- Never purchase software, equipment, or services as a condition of starting employment — universally a scam
- Treat confidentiality clauses on tasks before employment starts as a red flag
- Never pay for anything via cryptocurrency in an employment context — no legitimate employer accepts only Bitcoin
- Run all company domains through Scam Adviser and Scam Detector before engaging
- Check LinkedIn employee count — fake companies typically have 0–5 employees with AI-generated photos
- If an invoice has a 15-minute expiry window, stop and research immediately before paying

For Job Platforms (Internshala, LinkedIn, others)

- Implement domain age verification for employer accounts — all identified shells used very new domains
- Flag companies with no verifiable corporate registration number
- Establish a dedicated fraud reporting channel with committed response SLA
- Proactively alert all candidates who applied to any flagged company
- Ban cryptocurrency-only payment requirements from any advertised roles or tasks

For Law Enforcement (EFCC, CBI, Interpol)

- Investigate MutaEngine founder Bharti Kumari Singh and the domain mutaengine.cloud for financial fraud
- Submit confirmed Bitcoin wallet addresses for blockchain analysis and exchange-level KYC requests
- Issue takedown notices for mutaengine.cloud, pay.mutaengine.cloud, and all remaining zorvyn.* domains
- Coordinate with Hostinger to preserve access logs and identify registrant details behind privacy protection
- Engage cryptocurrency exchanges for wallet clustering analysis — identify aggregation wallet
- Pursue inter-jurisdictional cooperation: India (primary suspect location) + Nigeria + other victim geographies
- Report Bitcoin wallet addresses to bitcoinabuse.com for community flagging

12. Investigation Timeline

Date	Event
2 Apr 2026	Screening assessment invitation received from hr@zorvyn.io
3 Apr 2026	Offer letter received — signed by purported CEO Raj Kishor Pattnaik. INR 45,000 stipend + PPO up to INR 16 LPA
13 Apr 2026	Start date. Onboarding email, portal access, welcome kit ordered. Training task received — MutaCryptor purchase requested. Author does not purchase. Investigation begins.
14 Apr 2026	Bitcoin-only payment system discovered at pay.mutaengine.cloud. Wallet 1 captured. VRV Security correlation confirmed via Glassdoor. Report v1 published.
15 Apr 2026	Wallet 2 identified — rotation confirmed. Follow-up pressure email received from Mudiwa Mkonto threatening to block project access. Third wallet (bc1qvgka...) discovered via global.mutaengine.cloud.
18 Apr 2026	Infrastructure collapse — zorvyn.live NXDOMAIN. Email to mudiwamkonto@zorvyn.live bounces (DNS MX not found). workplace.zorvyn.live unreachable. Report v2 published.

13. Conclusion

The MutaCryptor Scam Network represents one of the most sophisticated and resource-intensive employment fraud operations documented to date. The combination of AI-generated fake employee identities, custom-built employee portal infrastructure, weeks-long trust-building onboarding, and a deliberately untraceable Bitcoin-only payment system places this operation firmly in the category of organised financial crime rather than opportunistic fraud.

The infrastructure collapse of zorvyn.live on 18 April 2026 — occurring during active investigation — confirms the operation is actively monitored and responsive to exposure, consistent with a professional fraud network rather than amateur actors. The teardown also confirms the operation is cyclical: the infrastructure will be rebuilt under a new shell company identity, likely already in development, targeting the next wave of job seekers.

The consistent and exclusive use of MutaCryptor across all documented fake company shells, combined with the Bitcoin-only payment design and the identification of founder Bharti Kumari Singh in Ghaziabad, India, collectively point toward a single controlling entity or tightly coordinated network. This report has established a documented, evidence-based foundation for law enforcement action.

This report is released under TLP: WHITE for unrestricted public distribution. Job seekers, platform operators, cybersecurity researchers, and law enforcement are encouraged to share this intelligence freely. The author welcomes additional corroborating reports and can be reached via cybernatesec.netlify.app.

14. References & Evidence Sources

- Glassdoor Community Forum — VRV Security scam report (February 2025)
- X/@rishiraamns — VRV Security investigation thread (December 2024)
- VRV Security Services official notice — vrvsecurityservices.com/about-us
- Reddit r/InternshipsIndia — Zorvyn scam discussion thread (April 2026)
- TakeOffTalent.com — Zorvyn FinTech analysis article (April 2026)
- Dilwado.com — Zorvyn hiring scam exposure article (April 2026)
- Grapevine.in — Multiple Zorvyn scam reports (April 2026)
- Wellfound — MutaEngine founder Bharti Kumari Singh, seed $10K Feb 2024, Ghaziabad
- Internshala — MutaEngine company listing (hiring since 2024, 0 candidates hired)
- ScamAdviser — zorvyn.io trust score 30.7/100 | vrvsecurity.in trust score 2/100 | mutaengine.cloud 76/100
- Scam Detector — zorvyn.io flagged as suspect website
- Author personal documentation — full 10-email chain, offer letter PDF, portal screenshots (April 2026)
- Bitcoin wallet addresses: bc1qqe3efq...eks50k | bc1q2h0q...em7s7 | bc1qvgka...ul84a
- NXDOMAIN evidence — zorvyn.live DNS collapse (18 April 2026)
- MutaCryptor payment screenshots — pay.mutaengine.cloud (14–16 April 2026)