# Hariharan M

hariharan.mathankumar@gmail.com | +91 9566714246 | Portfolio |
linkedin.com/in/hariharanmathan | github.com/misterxcrypt | medium.com/@misterxcrypt

## EXECUTIVE SUMMARY

Threat Intelligence Lead with 3+ years of experience in brand protection, dark web research, and cybercrime investigations. Built a money mule identification system that collected 100,000+ threat actor data points, helping government and financial institutions close nearly 90% of first-hop mule accounts within a day of creation. Skilled in OSINT, HUMINT, and dark web tradecraft, from sock-puppet operations to on-chain cryptocurrency tracing, with SOPs authored for team-wide use in persona management and brand-impersonation investigations. Looking to bring investigative, analyst-driven thinking to CTI teams delivering DRP, dark web monitoring, and threat actor/TTP intelligence that protects enterprise clients from emerging threats.

## PROFESSIONAL EXPERIENCE

**Threat Intelligence Lead,** Redhunt Labs Pvt Ltd — May 2025 – July 2026 | Remote

- **Internet-Scale Scanning Infrastructure:** Built an internet-scale scanning infrastructure capable of scanning the global IPv4 HTTPS attack surface in under 28 hours.
- **AI Security Research:** Conducted AI security research focused on asset discovery, exposure monitoring, fingerprinting, and secret leakage detection to support emerging AI attack surface management initiatives.
- **Digital Risk Protection (DRP):** Led Digital Risk Protection investigations for enterprise clients, uncovering phishing campaigns, brand impersonation, rogue applications, exposed infrastructure, and dark web threats.
- **SOP Authorship:** Authored standard operating procedures for sock-puppet/persona management and brand-impersonation investigations, standardizing OPSEC practices and investigation workflow across the CTI team.
- **Pre-Sales Security Consulting:** Partnered with pre-sales teams to demonstrate ransomware intelligence and dark web monitoring capabilities, contributing technical expertise during customer evaluations and solution discussions.
- **Phishing Detection Engineering:** Built an automated phishing and typosquatting detection system that discovers brand look-alike domains and forensically scores them for risk, replacing manual domain hunting with faster, explainable takedown decisions.
- **Telegram Intelligence Platform:** Designed a Telegram intelligence platform monitoring hundreds of channels/groups for threat intelligence collection and enrichment.
- **Client Reporting:** Redesigned ASM reporting by introducing separate executive and technical reports, improving stakeholder communication and assessment effectiveness.

**Cyber Threat Intelligence Analyst,** Saptang Labs Pvt Ltd — January 2023 – May 2025 | IIT MRP, India

- **Fraud & Phishing Intelligence:** Built a money mule identification system that collected and analyzed 100,000+ threat actor data points, 2,000+ malicious ad domains, and 1,000+ phishing sites, increasing real-time detection by 75% and helping government and financial institutions close nearly 90% of first-hop mule accounts within a day of creation.
- **Financial Scam Investigations:** Led OSINT, HUMINT, and social engineering investigations across a wide range of financial scams, cryptocurrency scams, lottery and gambling schemes, money mule networks, drawing on multiple sources and tools to uncover scammer tactics and infrastructure, potentially disrupting the operations.
- **Dark Web & Telegram Monitoring:** Monitored 20+ underground forums, dark web marketplaces, and Telegram channels, tracking ransomware groups and scam operations, mapping adversary TTPs to the MITRE ATT&CK framework, and conducting cybercrime ecosystem mapping, producing 80+ actionable intelligence reports.
- **Threat Actor Engagement (HUMINT & OPSEC):** Conducted TA engagements using proper OPSEC procedures to verify data leaks and understand the modus operandi of scams and frauds.
- **Brand Threat Monitoring:** Detected phishing sites, cloned APKs, and impersonation campaigns, including 2,000+ SEO-poisoned .gov.in pages and 10,000+ fraudulent bank customer-care numbers on YouTube.
- **Government Collaboration:** Supported law enforcement and regulatory investigations into financial fraud, terrorist funding, and extremist networks across Telegram and online forums, producing actionable intelligence referrals.

## INDEPENDENT RESEARCH & PERSONAL INITIATIVES

**Dark Web Research & On-Chain Analysis**

*Independent research, unaffiliated with any employer.*

- Independently tracked illicit services operating on the dark web, including carding platforms and child-exploitation (CSAM) infrastructure and conducted cryptocurrency and blockchain transaction tracing (on-chain analysis) to follow illicit fund flows linked to identified threat actors.

### Hacktivist & Disinformation Network Tracking

*Independent research, unaffiliated with any employer.*

- Collaborated with fellow OSINT researchers to track coordinated hacktivist collectives and disinformation campaigns across Telegram and social platforms during a period of regional geopolitical conflict, profiling propaganda dissemination channels and cross-platform attack infrastructure.

### Cybercrime Complaint & Case Management Platform

*Independent initiative, unaffiliated with any employer, built on personal time for a local cybercrime response unit.*

- Independently designed and deployed a WhatsApp-based complaint intake and case-tracking system for a local cybercrime response unit, streamlining citizen complaint collection and reducing manual case-handling efforts. The solution improved response times and enabled investigators to manage cases more efficiently.

## PROJECTS

**Telescribe** ↗ (Python, Telegram Intelligence)

- Telescribe builds an OSINT relationship map between Telegram channels, extracting t.me links shared in a channel's messages on the premise that a channel linking to another signals a real connection between them.
- Also ingests and AI-classifies a channel's messages for threat relevance, generating a summary and surfacing IOCs (domains, IPs, file hashes) to help CTI analysts quickly triage a source.

**Forums Bank** ↗ (Python, OSINT)

- Forums Bank is a curated intelligence repository that centralizes cybercrime forums, marketplaces, leak sites, and underground communities for streamlined threat research and intelligence collection.
- Contributed multiple dark web forums to the project's curated source list, expanding coverage across underground communities and marketplaces.

## CERTIFICATIONS

- ArcX Foundation Level Threat Intelligence Analyst
- Kase Scenarios Betrayal OSINT Training
- CISCO Introduction to Cyber Security
- Tracelabs OSINT Coach

## SKILLS

**THREAT INTELLIGENCE & INVESTIGATION**

Cyber Threat Intelligence, Digital Risk Protection, Dark Web Intelligence, OSINT, HUMINT, Attack Surface Management, MITRE ATT&CK Framework

**DARK WEB & FRAUD TRADECRAFT**

Sock-Puppet Operations, Cybercrime Ecosystem Mapping, Crypto On-Chain Analysis, Fraud & Financial Crime Intelligence, Certificate Transparency Log Monitoring

**TOOLS & PLATFORMS**

Shodan, Censys, VirusTotal, URLScan.io, SecurityTrails, FOFA, Maltego, Google Dorking

**TECHNICAL & DELIVERY**

Python, Selenium, MongoDB, Celery, Elasticsearch, Docker, Terraform, Cloud & Automation, Rapid MVP Prototyping

## EDUCATION

### B.Tech in Computer Science and Business Systems

2021 – 2025 | Coimbatore, India

*Sri Eshwar College of Engineering | CGPA: 8.61*

- **Leadership:** Organized cybersecurity seminars, workshops, and CTF events, mentoring students and fostering cybersecurity awareness within the college community.
- **Teamwork:** Actively participated in CTFs and hackathons with team NandBytes; organized college CTFs and trainings.

## AWARDS & ACHIEVEMENTS

- Published cybersecurity blogs on Medium, covering OSINT investigations, HackTheBox write-ups, and CVEs.
- Co-authored the Payment Gateway Security Handbook, covering the threat intelligence for payment gateways.
- Internal Smart Hack Challenge Hackathon Winner, 2022.
- Rajya Puraskar Award, 2019.