HARIHARAN M

hariharan.mathankumar@gmail.com +919566714246 My Portfolio

linkedin.com/in/hariharanmathan github.com/misterxcrypt medium.com/@misterxcrypt

PROFILE

Cybersecurity professional with 3+ years of experience in Cyber Threat Intelligence, Digital Risk Protection, and Attack Surface Management. Experienced in dark web investigations, phishing detection, OSINT operations, internet-scale security research, and threat intelligence automation. Proven track record of building intelligence platforms, conducting large-scale exposure analysis, and delivering actionable intelligence for enterprise clients.

PROFESSIONAL EXPERIENCE

Cyber Threat Intelligence Researcher, Redhunt Labs Pvt Ltd May 2025 – Present | 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):** Performed Digital Risk Protection assessments for enterprise clients across India and Southeast Asia, uncovering phishing infrastructure, brand abuse, executive impersonation, rogue applications, and dark web exposure impacting organizational security.
- **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:** Architected a phishing monitoring framework using typosquatting analysis, CT logs, domain intelligence, and threat feeds to improve early phishing detection.
- **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

- **Financial Scam Investigations:** Led OSINT and social engineering investigations into Southeast Asian scams, exposing scammer tactics and uncovering money laundering methods to improve fraud pattern detection.
- **Fraud & Phishing Intelligence:** Collected and analyzed 99,000+ scammer indicators, 2,000+ malicious ad domains, and 1,000+ phishing sites, disrupting fraud networks and phishing campaigns.
- **Threat Intelligence Automation:** Engineered a Python-based intelligence platform using Selenium, MongoDB, and Celery to automate scam data collection, increasing real-time threat detection by 75%.
- **Dark Web & Telegram Monitoring:** Monitored 20+ underground forums, dark web communities, and Telegram channels, tracking ransomware groups and scam operations while producing actionable intelligence reports.
- **Brand Threat Monitoring:** Developed detection capabilities for phishing sites, malicious advertisements, cloned APKs, impersonation pages, leaked documents, and compromised employee credentials.
- **Government Collaboration:** Worked with law enforcement and regulatory bodies on investigations involving financial fraud, terrorist funding, and organized cybercrime, supporting threat mitigation.
- **External Attack Surface Management (EASM):** Conducted attack surface assessments identifying exposed assets and credentials for client organizations, supporting new business acquisition and long-term customer engagements.

PROJECTS

Telescribe (Python, Telegram Intelligence)

- Telescribe is a Telegram intelligence platform designed for monitoring channels, groups, and threat-related discussions at scale through automated collection and keyword-based tracking.

- Built using Python with a modular architecture for channel onboarding, message collection, keyword monitoring, and intelligence enrichment to support cyber threat intelligence and digital risk investigations.

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.
- Developed using Python and web technologies to organize, categorize, and maintain searchable intelligence sources, enabling faster access to relevant threat actor ecosystems and dark web resources.

Zenblock (Firefox & Chrome Extension)
- Zenblock is a distraction-blocking browser extension that helps users maintain focus through website blocking, daily time limits, and scheduled access controls.
- Built for Firefox and Chrome with support for category-based filtering, focus mode, customizable block pages, and usage tracking.

Linux Rice Catalogue (React)
- Linux Rice Catalogue is a community-driven platform for discovering, sharing, and exploring Linux desktop customizations (rices) across multiple distributions, themes, and window managers.
- Developed as a modern web platform featuring advanced search, user submissions, screenshot galleries, wallpaper support, authentication workflows, and community-driven content management for Linux enthusiasts.

CERTIFICATIONS

- ArcX Foundation level Threat Intelligence Analyst
- CISCO Introduction to Cyber Security
- Kase Scenarios Betrayal Osint Training
- CISCO Networking Essentials

SKILLS

- Security Research
- Threat Intelligence
- Dark web Intelligence
- Product Innovation
- Open Source Intelligence
- Attack Surface Management
- Rapid MVP Prototyping
- Digital Risk Protection
- Cloud & Automation

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.
- **Coursework:** Operating Systems, Project Management, Financial Analytics, Marketing Research, Operations Research.

ADDITIONAL INFORMATION

Teamwork 2022 – present
- Actively participated in CTFs and hackathons with my team, NandBytes, also organized college CTFs and trainings.

Achievements
- Published cybersecurity blogs on Medium, covering OSINT Investigations, HackTheBox write-ups and CVEs.
- Internal Smart Hack Challenge Hackathon Winner 2022
- Rajya Puraskar Award 2019