



# Andrea Draghetti

HEAD OF CYBER THREAT INTELLIGENCE



+39 ND



drego85@draghetti.it



Bologna, Italy



andreadraghetti.it



in/andreadraghetti



drego85

## EDUCATION

### Bachelor's Degree in Computer Systems and Networks Security (SSRI)

*University of Milan, 2020*  
Thesis on the Evolution of  
Phishing: Analysis of  
phishing techniques and  
their development over  
time.

### High School Diploma in Electronics and Telecommunications

*I.T.I.S. Giordano Bruno,  
2004*

## LANGUAGES

- English: Intermediate -  
ESB Certificate
- Italian: Native

## INTERESTS

- Running
- Formula 1

## ABOUT ME

Cybersecurity analyst with over 9 years of experience in threat intelligence, antifraud, and malware analysis. Skilled in coordinating teams, developing custom tools, and managing enterprise clients in the banking, insurance, and energy sectors. Strong background in entrepreneurship and process automation, with proven ability to deliver effective threat detection and response strategies.

## PROFESSIONAL EXPERIENCE

### Head of Cyber Threat Intelligence / D3Lab SRL / 2019 - Present

- Lead and coordinate the Cyber Threat Intelligence and Antifraud/Phishing teams.
- Design and implement software tools and workflows to enhance phishing detection and takedown processes.
- Conduct threat analysis, data leak investigations, and malware reverse engineering for IoC extraction.
- Provide daily operational support, staff training, and troubleshooting for the team.
- Draft technical reports and threat assessments for enterprise clients (banks, insurance companies, energy providers, investment firms).

### Antifraud Analyst and Software Developer / D3Lab SRL / 2016 - 2018

- Monitoring, analyzing, and dismantling phishing campaigns targeting major Italian banks.
- Built internal tools (Python, PHP) for phishing detection, analysis automation, and client dashboards.

### Contributor / BackBox Linux / 2010 - 2019

- Tested and validated the Linux security distribution.
- Built and maintained Debian packages for penetration testing tools.
- Provided technical support and collaborated with the open-source community.

### Dealer / Draghetti SNC / 2005 - 2016

- Managed a Vodafone Italy franchise store, overseeing operations, administration, and staff.
- Handled customer relations, conflict resolution, and commercial risk management.

## KEY PROJECTS

- Phishing Army – Phishing blocklist serving over 500,000 monthly users
- Over Security – Cyber threat intelligence news aggregator and podcast.
- meioc – Mail Extractor Indicator of Compromise (IoC).
- tosint – OSINT tool for extracting data from Telegram bots and channels.

## SKILLS

- Cybersecurity & Threat Intelligence: Phishing takedown, antifraud, malware analysis, data leak investigation, IoC extraction.
- Bug Bounty & Vulnerability Research: Responsible disclosures with Telegram, TIM, Vodafone, ilPost, and others.
- Software Development: Python, PHP, MySQL, web scraping, process automation, dashboard/web tools.
- Operating Systems & Tools: macOS, Linux, HTML, JavaScript.