

# Michele Campobasso

PhD in Information Security @ Eindhoven University of Technology

📍 Bologna, Italy 📞 +39 340 07 04 237 📧 m.campobasso@tue.nl



## about me

Computer scientist with an unusual interest for social relations. I am often called optimistic, but I consider myself realistic. I believe that many problems need just a different approach to be solved. I am the kind of guy that wonders 'why' a thing has always been like that, often between 10PM and 3AM.

## personal

pronouns: he/him  
nationality: Italian

## languages

Italian: mother tongue  
English: professional proficiency

## areas of specialization

Threat modeling,  
emerging threats,  
underground market  
investigation, threat  
quantification,  
penetration testing

## interests

Biking, go-karts, hiking,  
organizing social  
events, on-the-road  
travels, fixing 'broken'  
electronics, cooking  
Italian & exotic food, my  
nerdy YouTube feed

## RESEARCH OVERVIEW & IMPACT

- EXPERTISE IN: **underground forum marketplaces** and their **impact** in the threat landscape [2], **emerging threats** and **threat modeling** [6], underground community infiltration, **stealth** data collection [3], **attacker preferences** and **cyber threat quantification** [1]
- RESEARCH ON EMERGENT THREAT [6] instrumental to **international investigation led by the Dutch National Police, FBI & EUROPOL**, leading to hundreds of arrests worldwide & market shutdown in a massive law enforcement operation ([press release](#)).
- CONTRIBUTION ON ACCESS-AS-A-SERVICE [4] was **presented to the U.S. Department of Commerce**; NSO Group was included as a company threatening the US national security ([press release](#)).
- LARGE INDUSTRY & MEDIA ATTENTION ([Troy Hunt](#), [Recorded Future on Genesis Market](#), [local media](#))
- AWARDS: **Best Dutch Cybersecurity Paper 2024**, runner up [1], Distinguished **Paper** with Artifacts [5].
- EXPLOIT PREDICTION SCORING SYSTEM (EPSS) special interest group member and contributor ([link](#)).

## WORK EXPERIENCE

2019-2022	<b>Head of lab activities for Offensive Computer Security</b> ORGANIZING HANDS-ON LAB SESSIONS AND MANAGING 150+ STUDENTS <i>Eindhoven University of Technology</i> 📍
2019-2024	<b>Supervisor and coordinator of scientific projects at the MSc level</b> 9 GROUPS, 35 STUDENTS OA – THREAT INTEL EXTRACTION, MALWARE ANALYSIS <i>Eindhoven University of Technology</i> 📍
2019-2023	<b>Analyst of underground cybercriminal markets: infiltration, stealth monitoring, threat modeling, and activity estimation</b> OBTAIN ACCESS TO SEGREGATED MARKETS; AUTOMATED, STEALTH DATA EXTRACTION WITH TAILORED, CUSTOM CREATED CRAWLERS; EMPIRICAL AND STATISTICAL METHODS, UNDERGROUND INVESTIGATIONS <i>Eindhoven University of Technology</i> 📍
2019-2024	<b>Doctorate in Information Security - Specialty: Cybercrime Ecosystem</b> <i>Eindhoven University of Technology</i> 📍
May-Sep 2016	<b>Internship: Junior Backend Developer and Beta Tester</b> <i>GetConnected S.r.l.</i> 📍
Mar-Jun 2015	<b>Internship: Junior Developer</b> <i>AltaVia S.r.l.</i> 📍

## EDUCATION

2019-2024	<b>Doctorate in Information Security – Specialty in Cybercrime Ecosystem</b> Thesis title: Understanding and Characterizing the Cybercriminal Ecosystem Enabling Attack Innovation at Scale <i>Eindhoven University of Technology</i>
2016-2019	<b>Master in Computer Science and Engineering</b> Thesis title: CARONTE: a Crawler for Adversarial Resources Over Non-Trusted, high-profile Environments <i>Alma Mater Studiorum - University of Bologna</i>
2011-2016	<b>Bachelor in Computer Engineering</b> <i>Alma Mater Studiorum - University of Bologna</i>

## INVITED TALKS

May 2023	<b>'Not all cybercrime is boring if you know what to look for'</b> – UNDERGROUND THREAT SOURCES, CYBER THREAT QUANTIFICATION @ <i>INTERSET 2023, The Hague, NL</i>
Mar 2023	<b>“Do we have an agreement?": Exploiting Trust Mechanisms in Cybercrim. Undergr. Mark. to Derive Attacker Pref. and Estimate Threat Levels'</b> – UNDERGR. THREAT SOURCES, CYBER THREAT QUANTIF. @ <i>University of Bologna, Bologna, IT</i>
May 2022	<b>'Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale'</b> – EMERGING THREATS, THREAT MODELING, CYBER THREAT QUANTIFICATION @ <i>INTERSET 2022, Enschede, NL</i>
Dec 2021	<b>'The Role of the Criminal Economy on the Emergence of User Imp. at Scale'</b> – EMERG. THRS., THRT. MOD. @ <i>NYU Computational Disinformation Sympos., Online</i>
Feb 2021	<b>'Not all threat (actors) are the same: a multidisciplinary take on cybercrime proliferation'</b> – EMERG. THRS., THRT. MOD. @ <i>Dutch Police Cybercrime Team, Online</i>
Nov 2020	<b>'Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale'</b> – EMERGING THREATS, THREAT MODELING @ <i>ASML, Eindhoven, NL</i>
Mar 2020	<b>'Myth-busting the underground: a journey into the (often un)organized cyber-crime'</b> – UNDERGROUND ECOSYSTEM @ <i>University of Bologna, Bologna, IT</i>

🐦 @alpha\_centauri3  
📺 michelecampobasso

## TECHNICAL CYBERSECURITY EXPERIENCE

2019-2022	<b>Head of lab activities for Offensive Computer Security at Eindhoven University of Technology</b> ORGANIZING HANDS-ON LAB SESSIONS AND MANAGING 150+ STUDENTS
2019-2021	<b>Malware analysis and reverse engineering</b> EXPERIENCE WITH GHIDRA & GDB MATURED WITH CTFs AND ACADEMIC RESEARCH
2018-2023	<b>Tool creation for stealth data extraction</b> BROWSER INSTRUMENTATION, HUMAN BEHAVIOR MODELING, DATA PARSING ON THE FLY
2016-2020	<b>HackTheBox CTFs</b> BEST RANKING GLOBALLY ON THE PLATFORM: 187, COMPLETION SCORE OF 76%
2019-2020	<b>HackTheBox write-ups blog</b> CO-AUTHOR OF A <a href="#">BLOG</a> CONTAINING DETAILED WRITE-UPS OF RETIRED BOXES FROM THE PLATFORM HACKTHEBOX
2017-2019	<b>IO NetGarage</b> REVERSE ENGINEERING & BINARY EXPLOITATION. BASIC EXPLOIT CRAFTING SKILLS
2018-2019	<b>Various CTF challenges</b> AS A MEMBER OF THE UNIVERSITY OF BOLOGNA'S HACKING TEAM ULISSELABBO

## CERTIFICATIONS

Nov 2024	<b>Tech Against Terrorism Europe – TCO Regulation</b> <i>Requirements, obligations and recommendations for IT professionals to counter terrorist content; identification and assessment of terrorist content; moderation mechanisms; tools for identification and disruption of terrorist content.</i> <a href="#">TECH AGAINST TERRORISM EUROPE</a> – <a href="#">CERTIFICATE LINK</a>
----------	---

## FULL LIST OF PUBLICATIONS

Aug 2023	<b>[1] Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale (<a href="#">paper</a>)</b> . <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">LUCA ALLODI</a> ; <i>32<sup>nd</sup> USENIX Security Symposium (USENIX Security 2023)</i> , Los Angeles, USA 📍
Jul 2023	<b>[2] You Can Tell a Cybercriminal by the Company they Keep: A Framework to Infer the Relevance of Underground Communities to the Threat Landscape (<a href="#">paper</a>)</b> . <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">LUCA ALLODI</a> ; <i>The 22<sup>nd</sup> Workshop on the Economics of Information Security (WEIS 2023)</i> , Geneva, Switzerland 📍
Nov 2022	<b>[3] THREAT/crawl: a Trainable, Highly-Reusable, and Extensible Automated Method and Tool to Crawl Criminal Underground Forums (<a href="#">paper</a>)</b> . <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">LUCA ALLODI</a> ; <i>The 17<sup>th</sup> Symposium on Electronic Crime Research (APWG eCrime 2022)</i> , online
Feb 2022	<b>SAIBERSOC: A Methodology and Tool for Experimenting with Security Operation Centers (<a href="#">paper</a>)</b> . <a href="#">MARTIN ROSSO</a> , <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">GANDGUULGA GANKHUYAG</a> , <a href="#">LUCA ALLODI</a> ; <i>Digital Threats: Research and Practice</i> .
Mar 2021	<b>[4] A Primer on the Proliferation of Offensive Cyber Capabilities (<a href="#">paper</a>)</b> . <a href="#">WINNONA DESOMBRE</a> , <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">LUCA ALLODI</a> , <a href="#">JAMES SHIRES</a> , <a href="#">JD WORK</a> , <a href="#">ROBERT MORGUS</a> , <a href="#">PATRICK HOWELL O'NEILL</a> , <a href="#">TREY HERR</a> ; <i>In-Depth Research &amp; Reports</i> , Atlantic Council
Feb 2022	<b>[5] SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers (<a href="#">paper</a>)</b> . <a href="#">MARTIN ROSSO</a> , <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">GANDGUULGA GANKHUYAG</a> , <a href="#">LUCA ALLODI</a> ; <i>The 36<sup>th</sup> Annual Computer Security Applications Conference (ACSAC 2020)</i> , online Distinguished Paper with Artifacts
Nov 2020	<b>[6] Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale (<a href="#">paper</a>)</b> . <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">LUCA ALLODI</a> ; <i>2020 ACM SIGSAC Conference on Computer and Communications Security (CCS 2020)</i> , online Mentioned in ACM CCS 2020 Highlights
Jul 2019	<b>CARONTE: a Crawler for Adversarial Resources Over Non-Trusted, high-profile Environments (<a href="#">paper</a>)</b> . <a href="#">MICHELE CAMPOBASSO</a> , <a href="#">LUCA ALLODI</a> ; <i>The 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&amp;PW) - 1st Workshop on Attackers and Cyber-Crime Operations</i> , Stockholm, Sweden 📍