Michele **Campobasso**

PhD in Information Security @ Eindhoven University of Technology

Bologna, Italy @ 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

@alpha_centauri3
michelecampobasso

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	**Head of lab activities for Offensive Computer Security** Organizing hands-on lab sessions and managing 150+ students *Eindhoven University of Technology*
2019-2024	**Supervisor and coordinator of scientific projects at the MSc level** 9 groups, 35 students OA – Threat intel extraction, malware analysis *Eindhoven University of Technology*
2019-2023	**Analyst of underground cybercriminal markets: infiltration, stealth monitoring, threat modeling, and activity estimation** Obtain access to segregated markets; automated, stealth data extraction with tailored, custom created crawlers; empirical and statistical methods, underground investigations *Eindhoven University of Technology*
2019-2024	**Doctorate in Information Security - Specialty: Cybercrime Ecosystem** *Eindhoven University of Technology*
May-Sep 2016	**Internship: Junior Backend Developer and Beta Tester** *GetConnected S.r.l.*
Mar-Jun 2015	**Internship: Junior Developer** *AltaVia S.r.l.*

Education

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

Invited Talks

May 2023	**'Not all cybercrime is boring if you know what to look for'** – Underground threat sources, Cyber Threat Quantification @ *INTERSCT 2023, The Hague, NL*
Mar 2023	**'"Do we have an agreement?": Exploiting Trust Mechanisms in Cybercriminal Underground Markets to Derive Attacker Preferences and Estimate Threat Levels'** – Underground threat sources, Cyber Threat Quantification @ *Alma Mater Studiorum - University of Bologna, Bologna, IT*
May 2022	**'Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale'** – Emerging threats, Threat modeling, Cyber Threat Quantification @ *INTERSCT 2022, Enschede, NL*
Feb 2021	**'Not all threat (actors) are the same: a multidisciplinary take on cybercrime proliferation'** – Emerging threats, Threat modeling @ *Dutch Police Cybercrime Team, Online*
Nov 2020	**'Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale'** – Emerging threats, Threat modeling @ *ASML, Eindhoven, NL*
Mar 2020	**'Myth-busting the underground: a journey into the (often un)organized cybercrime'** – Underground ecosystem @ *Alma Mater Studiorum - University of Bologna, Bologna, IT*

Technical Cybersecurity experience

2019-2022	**Head of lab activities for Offensive Computer Security at Eindhoven University of Technology** Organizing hands-on lab sessions and managing 150+ students
2019-2021	**Malware analysis and reverse engineering** Experience with Ghidra & GDB matured with CTFs and academic research
2018-2023	**Tool creation for stealth data extraction** Browser instrumentation, human behavior modeling, data parsing on the fly
2016-2020	**HackTheBox CTFs** Best ranking globally on the platform: 187, completion score of 76%
2019-2020	**HackTheBox write-ups blog** Co-author of a blog containing detailed write-ups of retired boxes from the platform HackTheBox
2017-2019	**IO NetGarage** Reverse engineering & binary exploitation. Basic exploit crafting skills
2018-2019	**Various CTF challenges** As a member of the University of Bologna's hacking team UlisseLabBO

Certifications

Nov 2024	**Tech Against Terrorism Europe – TCO Regulation** *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.* Tech Against Terrorism Europe – Certificate link

Full list of Publications

Aug 2023	**[1] Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale (paper).** Michele Campobasso, Luca Allodi; *32nd USENIX Security Symposium (USENIX Security 2023), Los Angeles, USA*
Jul 2023	**[2] You Can Tell a Cybercriminal by the Company they Keep: A Framework to Infer the Relevance of Underground Communities to the Threat Landscape (paper).** Michele Campobasso, Luca Allodi; *The 22nd Workshop on the Economics of Information Security (WEIS 2023), Geneva, Switzerland*
Nov 2022	**[3] THREAT/crawl: a Trainable, Highly-Reusable, and Extensible Automated Method and Tool to Crawl Criminal Underground Forums (paper).** Michele Campobasso, Luca Allodi; *The 17th Symposium on Electronic Crime Research (APWG eCrime 2022), online*
Feb 2022	**SAIBERSOC: A Methodology and Tool for Experimenting with Security Operation Centers (paper).** Martin Rosso, Michele Campobasso, Gandguulga Gankhuyag, Luca Allodi; *Digital Threats: Research and Practice.*
Mar 2021	**[4] A Primer on the Proliferation of Offensive Cyber Capabilities (paper).** Winnona DeSombre, Michele Campobasso, Luca Allodi, James Shires, JD Work, Robert Morgus, Patrick Howell O'Neill, Trey Herr; *In-Depth Research & Reports, Atlantic Council*
Feb 2022	**[5] SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers (paper).** Martin Rosso, Michele Campobasso, Gandguulga Gankhuyag, Luca Allodi; *The 36th Annual Computer Security Applications Conference (ACSAC 2020), online* Distinguished Paper with Artifacts
Nov 2020	**[6] Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale (paper).** Michele Campobasso, Luca Allodi; *2020 ACM SIGSAC Conference on Computer and Communications Security (CCS 2020), online* Mentioned in ACM CCS 2020 Highlights
Jul 2019	**CARONTE: a Crawler for Adversarial Resources Over Non-Trusted, high-profile Environments (paper).** Michele Campobasso, Luca Allodi; *The 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) - 1st Workshop on Attackers and Cyber-Crime Operations, Stockholm, Sweden*

Bologna, Italy @ m.campobasso@tue.nl