# MARCUS FELIPE BOTACIN

https://scholar.google.com.br/citations?user=Y8JHVbcAAAAJ
mfbotacin@{gmail.com, inf.ufpr.br} - https://marcusbotacin.github.io/
https://twitter.com/marcusbotacin - https://github.com/marcusbotacin

## EDUCATION

**Federal University of Paraná (UFPR), Brazil** *2017 - December/2021*
PhD in Computer Science: "*On the Malware Detection Problem: Challenges and new Approaches*"
Advisor: André Ricardo Abed Grégio

**University of Campinas (UNICAMP), Brazil** *2015 - 2017*
Master in Computer Science: "*Hardware-Assisted Malware Analysis*"
Advisor: Paulo Lício de Geus

**University of Campinas (UNICAMP), Brazil** *2010 - 2015*
Bachelor in Computer Engineering: "*Malware detection via syscall patterns identification*"
Advisor: Paulo Lício de Geus

## INTERNATIONAL EXPERIENCE

**University of Florida** NSF US-Brazil Collaboration
*Visiting Researcher hosted by Prof. Daniela Oliveira (UF, Gainesville)* *August/2018 and May/2019*

**Friedrich-Alexander-Universität Erlangen-Nürnberg** DAAD Germany-Brazil Collaboration
*Visiting Researcher hosted by: Prof. Tilo Muller (FAU, Erlangen)* *November/2018*

## RESEARCH INTERESTS

Malware Analysis, Evasion, and Detection
Sandbox Development and Antivirus Operation
Hardware-Assisted Security Solutions
Reverse Engineering

## AWARDS

Best Master Dissertation - 1st place - Brazilian Computer Society - 2018
Best Undergraduate Research Paper (co-author)- 1st place - Brazilian Computer Society - 2018
Best PhD Thesis Candidate - Brazilian Computer Society - 2022* (TBD)
Travel Grant - Student Diversity Grant - USENIX ENIGMA - 2019

## PRIZES

Participation in the Machine Learning-based malware evasion challenge (mlsec.io).

Defenders 2021: 1st place
Defenders 2020: 2nd place
Attackers 2021: 1st place
Attackers 2019: 2nd place
Attackers 2020: 1st place

## DEVELOPMENT PROJECTS

**Corvus: Public, Online Malware Analysis Sandbox** - https://corvus.inf.ufpr.br/

## FEATURED TALKS

"*Does Your Threat Model Consider Country and Culture? A Case Study of Brazilian Financial Malware to show that it Should!*" - USENIX ENIGMA 2021 - https://www.youtube.com/watch?v=5mrEJ83rBDY

## ACADEMIC COMMUNITY SERVICES

Program Committee member for USENIX Security 2022
Artifact Evaluation Committee for USENIX Security 2020 and USENIX WOOT 2020
Ad-hoc reviewer for ACM CSUR, IEEE TIFS, ELSEVIER Comp&Sec, and others.
External reviewer for the Brazilian Security Symposium (SBSeg) - 2015 to 2021

## PUBLICATION SUMMARY

- 11 papers published in international journals
  - Including top venues, such as ACM CSUR, ACM TOPS, IEEE TDSC, and ELSEVIER Computers & Security
- 7 papers in International conferences
  - Including reputable venues, such as DIMVA and ARES
- 12 papers in Brazilian conferences
- 2 book chapters (in Portuguese)

## SELECTED PUBLICATIONS

### Research on Brazilian Malware

"*One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware*" - ACM TOPS 2021 - https://dl.acm.org/doi/10.1145/3429741

"*The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study*" - ACM ARES 2019 - https://dl.acm.org/doi/10.1145/3339252.3340103

### Research on Malware Research Methods

"*Challenges and pitfalls in malware research*" - ELSEVIER Computers & Security 2021 - https://www.sciencedirect.com/science/article/pii/S0167404821001115

"*We need to talk about antiviruses: challenges & pitfalls of AV evaluations*" - ELSEVIER Computers & Security 2020 - https://www.sciencedirect.com/science/article/pii/S0167404820301310

"*Understanding uses and misuses of similarity hashing functions for malware detection and family clustering in actual scenarios*" - ELSEVIER Digital Investigation 2021 - https://www.sciencedirect.com/science/article/abs/pii/S266628172100

### Research on Sandbox Development

"*The other guys: automated analysis of marginalized malware*", Springer Journal of Computer Virology and Hacking Techniques 2018 - https://link.springer.com/article/10.1007/s11416-017-0292-8

"*Enhancing Branch Monitoring for Security Purposes: From Control Flow Integrity to Malware Analysis and Debugging*" - ACM Transactions on Privacy and Security 2018 - https://dl.acm.org/doi/10.1145/3152162

### Research on Hardware-Assisted Security

"*Who Watches the Watchmen: A Security-focused Review on Current State-of-the-art Techniques, Tools, and Methods for Systems and Binary Analysis on Modern Platforms*". ACM Computing Surveys (2018)

"*Near-Memory In-Memory Detection of Fileless Malware*" - ACM MEMSYS 2020 - https://dl.acm.org/doi/10.1145/3422575.3422775

### Research on Applied Security

"*On the Security of Application Installers and Online Software Repositories*" - DIMVA 2020 - https://link.springer.com/chapter/10.1007/978-3-030-52683-2_10