MARCUS FELIPE BOTACIN

https://scholar.google.com/citations?user=Y8JHVbcAAAAJ
mfbotacin@gmail.com - https://marcusbotacin.github.io/
https://twitter.com/marcusbotacin - https://github.com/marcusbotacin

EMPLOYMENT

Assistant Professor — ***09/2024 - TBD***
Texas A&M University (TAMU), USA
Visiting Assistant Professor — ***08/2022 - 08/2024***
Texas A&M University (TAMU), USA
Lecturer — ***2021/2***
Federal University of Paraná (UFPR), Brazil

EDUCATION

Ph.D. in Computer Science — ***2017 - 2021***
Federal University of Paraná (UFPR), Brazil
Thesis Title: "*On the Malware Detection Problem: Challenges and new Approaches*"
Advisor: Prof. Dr. André Ricardo Abed Grégio (UFPR)
CoAdvisor: Prof. Dr. Paulo Lício de Geus (UNICAMP)
Thesis Committee: Ph.D. Leigh Metcalf (CERT, Carnegie Mellon University), Ph.D. Leyla Bilge (Norton LifeLock), Prof. Dr. Daniel Oliveira (UFPR)
M.Sc. in Computer Science — ***2015 - 2017***
University of Campinas (UNICAMP), Brazil
Dissertation Title: "*Hardware-Assisted Malware Analysis*"
Advisor: Prof. Dr. Paulo Lício de Geus (UNICAMP)
CoAdvisor: Prof. Dr. André Ricardo Abed Grégio (UFPR)
Dissertation Committee: Prof. Dr. Carlos Maziero (UFPR), Prof. Dr. Sandro Rigo (UNICAMP)
B.Sc. in Computer Engineering — ***2010 - 2015***
University of Campinas (UNICAMP), Brazil
Final Project Title: "*Malware detection via syscall patterns identification*"
Advisor: Prof. Dr. Paulo Lício de Geus (UNICAMP)

INTERNATIONAL RESEARCH EXPERIENCE

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

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

RESEARCH INTERESTS

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

(CO)ADVISED UNDERGRADUATE STUDENTS

Lucas Baganha Galante (UNICAMP, 2017-2019) - Linux Malware and ML-based malware detection.
Giovanni Bertão (UNICAMP, 2017-2019) - Large-scale malware repositories and application crawling.
Vitor Falcão da Rocha (UNICAMP, 2016-2017) - Anti-forensics and malware anti-analysis.
Raphael Machinicki (UFPR, 2019-2020) - Analysis of Android apps' operations.
Felipe Duarte Domingues (UFPR/UNICAMP, 2019-2021) - Antivirus' operations.

ACADEMIC AWARDS

Top-3 Best PhD Thesis in Security - Brazilian Computer Society - 2022
Best PhD Thesis - Department of Informatics/UFPR - 2022
Best Master Dissertation in Security - 1st place - Brazilian Computer Society - 2018
Best Master Dissertation - Institute of Computing/UNICAMP - 2018
Best Undergraduate Security Research Paper (co-author)- 1st place - Brazilian Computer Society - 2018
Travel Grant - Student Diversity Grant - USENIX ENIGMA - 2019

CONTESTS 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

"*Why Is Our Security Research Failing? Five Practices to Change!*" - USENIX ENIGMA 2023 - https://www.usenix.org/conference/enigma2023/presentation/botacin
"*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

Guest Editor for ACM DTRAP Special Issue on Non-conventional Malware (2023).
Program Committee member for USENIX Security 2022 and 2023.
Artifact Evaluation Committee for the Journal of Systems Research (JSys).
Artifact Evaluation Committee for USENIX Security 2020 and USENIX WOOT 2020.
Artifact Evaluation Committee for Journal of Systems Research (JSys)
Ad-hoc reviewer for ACM CSUR, IEEE TIFS, ELSEVIER Comp&Sec, and others.
External reviewer for the Brazilian Security Symposium (SBSeg) - 2015 to 2022.

PUBLICATION SUMMARY

- 15 papers published in international journals
  - Including top venues, such as ACM CSUR, ACM TOPS, and IEEE TDSC.
- 10 papers in International conferences
  - Including reputable venues, such as DIMVA and ACM ARES.
- 12 papers in Brazilian conferences (SBSeg).
- 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

“*Why do we need a theory of maliciousness*” **- Springer Information Security Conference (ISC) 2022 -** `https://link.springer.com/chapter/10.1007/978-3-031-22390-7_22`

“*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

“*Dissecting Applications Uninstallers and Removers: Are They Effective?*” **- Springer Information Security Conference (ISC) 2022 -** `https://link.springer.com/chapter/10.1007/978-3-031-22390-7_20`

“*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`

Research on Antivirus Internals

“*AntiViruses under the microscope: A hands-on perspective*” **- Elsevier Computers & Security 2021 -** `https://www.sciencedirect.com/science/article/pii/S0167404821003242`