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 *11/2024 - TBD*
Texas A&M University (TAMU), USA
Visiting Assistant Professor *10/2022 - 10/2024*
Texas A&M University (TAMU), USA
Lecturer *2021/2*
Federal University of Paraná (UFPR), Brazil

OTHER PROFESSIONAL ACTIVITIES

Scientific Board Advisor *3/2023 - 8/2024*
CYMDALL -https://www.cymdall.com/**, Israel**
Security Startup developing hardware-assisted detection mechanisms.

Scientific Board Advisor *8/2024 - 8/2024*
AppThreat -https://appthreat.com/**, UK**
Security company developing open-source tools.

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

RESEARCH GRANTS

NSF SaTC: CORE: Small: An evaluation framework and methodology to streamline Hardware Performance Counters as the next-generation malware detection system - PI - 2024=2026 - $ 523.415,00 - https://www.nsf.gov/awardsearch/showAward?AWD_ID=2327427&HistoricalAwards=false

CURRENTLY ADVISED STUDENTS (AT TAMU): 5

Sidharth Anil - MSc - Project-Based (2023/5-In Progress)
Soumyajyoti Dutta - MSc - Project-Based (2023/5-In Progress)
Snehith Bikumandla - MSc - Project-Based (2023-In Progress)
John Ammon - Undergrad - Project-based (2023/5-In Progress)
Uros Stanic - Undergrad -Faculty of Technical Sciences of Novi Sad (Serbia) - Computer Science Student Advancement Program (CSSAP) Summer Internship - (2023/Summer)

PREVIOUSLY ADVISED STUDENTS (AT TAMU): 2

Parul Damahe - MSc - Project-Based (2023-In Progress)
Pranav Taukari - MSc - Project-Based (2023-In Progress)

(CO)ADVISED UNDERGRADUATE STUDENTS (IN BRAZIL): 5

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	**Attackers 2021: 1st place**	**Attackers 2020: 1st place**
Defenders 2020: 2nd place	**Attackers 2019: 2nd 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.youtube.com/watch?v=7XUKwSExJGO&t=4s&pp=ugMICgJwdBABGAE%3D

"***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

"***All You Always Wanted to Know About Antiviruses*** " **- HackInTheBox 2023 -** https://conference.hitb.org/hitbsecconf2023ams/session/commsec-all-you-always-wanted-to-know-about-antiviruses/ **-** https://www.youtube.com/watch?v=fnexx1Ek168

MEDIA COVERAGE

NSF SaTC HPC grant award on TAMU website: https://engineering.tamu.edu/news/2023/08/innovative-approach-detecting-malware-through-hardware-integrated-protection.html

ACADEMIC COMMUNITY SERVICES

National Science Foundation (NSF) Panelist.
Guest Editor for ACM DTRAP Special Issue on Non-conventional Malware (2023).
Program Committee member for ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2024
Program Committee member for ACM Conference on Computer and Communications Security (CCS) 2023 (Software Track).
Program Committee member for Network and Distributed Systems Security (NDSS) Conference 2024.
Program Committee member for Conference on Computer and Communications Security (CCS) 2023 (Software Track).
Program Committee member for USENIX Security 2022, 2023, and 2024.
Program Committee member for ACM Annual Computer Security Applications Conference (ACSAC 2023).
Program Committee member for International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2023).
Program Committee for International Workshop on Re-design Industrial Control Systems with Security (RICSS), EuroS&P23
Program Committee for The 15th International Workshop on Cyberspace Security and Artificial Intelligence (CAI-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)
External reviewer for the Brazilian Security Symposium (SBSeg) - 2015 to 2022.
Ad-hoc reviewer for 16 different journals:

- **ACM Computing Surveys (CSUR)**
- **ACM Digital Threats: Research and Pratice (DTRAP)**
- **Cell: Patterns**
- **Elsevier Computers Security**
- **Elsevier Computers in Human Behavior**
- **Elsevier Forensic Science International: Digital Investigation (Digital Investigation)**
- **IEEE Open Journal of the Computer Society (OJCS)**
- **IEEE Transactions on Dependable and Secure Computing (TDSC)**
- **IEEE Transactions on Information Forensics and Security (TIFS)**
- **IEEE Transactions on Mobile Computing (TMC)**
- **IEEE Transactions on Emerging Topics in Computing (TETC)**
- **Springer Artificial Intelligence Review**
- **Springer Computing**
- **Springer International Journal of Information Security**
- **Springer Journal of SuperComputing**
- **Wiley Journal of Software: Evolution and Process**

83 reviews currently acknowledged in WebofScience (WoS):
https://www.webofscience.com/wos/author/record/2102545

PUBLICATION SUMMARY

- **16 papers published in international journals**
  - **Springer Journal in Computer Virology: 4**
  - **ACM Transactions on Privacy and Security (TOPS): 3**
  - **Elsevier Computers and Security: 3**
  - **Elsevier Expert Systems With Applications (ESWA): 2**

  - **ACM Computing Surveys (CSUR): 1**
  - **ACM Digital Threats: Research and Practice (DTRAP): 1**
  - **IEEE Transactions on Dependable and Secure Computing (TDSC): 1**
  - **Elsevier Digital Investigation: 1**
- **12 papers in International conferences**
  - **ACM Reversing and Offensive-oriented Trends Symposium (ROOTS): 3**
  - **Springer Information Security Conference (ISC): 3**
  - **Springer Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 1**
  - **ACM Availability, Reliability and Security (ARES): 1**
  - **ACM Conference on Code Generation and Optimization (CGO): 1**
  - **ACM Memory Systems (MEMSYS): 1**
  - **IEEE Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC): 1**
  - **Workshop on Offensive Technologies (WOOT): 1**
- **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

Research on Code Obfuscation

"***A Game-Based Framework to Compare Program Classifiers and Evaders***" **- ACM CGO 2023 -** https://dl.acm.org/doi/10.1145/3579990.3580012