RAFAEL SALEMA MARQUES

salemarsm@gmail.com Phone: +44 7534867398
http://www.creativecode.com.br/rafael-salema-marques
https://www.linkedin.com/in/rafael-salema-marques-msc-987bb88b/

Decisive and focused Cybersecurity professional with an extensive history of threat predictions malware analysis and reverse engineering. Outstanding technical, communication, interpersonal, analytical, and problem-solving skills.

- Threat Hunter
- Cybersecurity Researcher
- Artificial Immune Systems
- Cyber Intelligence Analyst
- Malware Reverse Engineering
- Leadership

PROFESSIONAL EXPERIENCE

Wolverhampton Cyber Research Institute WCRI, Wolverhampton, United Kingdom **2019 – Present**
University of Wolverhampton.

PhD, Cybersecurity Jun. 2019 – Present

- Researching data exfiltration and covert channels (C2) detection.
- Giving lectures related to cybersecurity at the University of Wolverhampton.

Brazilian Air Force Intelligence Center, Brasília, Brazil **2018 – 2019**
Brazilian Air Force Cybersecurity Intelligence Division.

Chief, Red Team Jan. 2018 – Jun 2019

- Responsible for conducting the operations of the Brazilian Air Force Red Team.
- Conduct penetration test on intranet networks and web applications.
- Execute cyber forensics investigations.
- Development of tools and malicious code to support Red Team activities.
- Analyze and evaluate cyber threats.

2º/1º Command and Control Group (21GCC), Canoas, Brazil **2015 – 2018**
Brazilian Air Force Squad focused on Command and Control Infrastructure of military operations.

Commander Jan. 2015 – Jan. 2017

- Responsible for conducting the operations of a strategic squad of Brazilian Air Force (Manage a team of 75 military personnel).
- Cybersecurity Evangelist of Brazilian Air Force Command and Control Squads, making lectures and training about Cybersecurity awareness.
- Team Resource Management (TRM) Instructor of Brazilian Airspace Control Department (DECEA). The aims of TRM are to develop positive attitudes and behaviors towards teamwork skills and human performance, helping to reduce the number or minimize the impact of teamwork-related errors.
- Development of cyber artifacts.

Aeronautics Institute of Technology (ITA), São José dos Campos, Brazil **2014 - 2015**
Brazilian renowned University of engineering globally recognized for talents exportation.

MSc, Computer Engineering (Artificial immune systems, Multi-Agent systems) Jan. 2014 – Dec. 2015

- Development of MADEC (Multi-Agent Data Exfiltration Catcher) architecture. The architecture is supported by immunological metaphors, and the goal is to identify data exfiltration activities performed by rootkits, even when those are able to hide malicious traffic from the infected host.
- The developer of Mabouia, the world first full functional Ransomware that target MAC OSX (Proof of concept, source code not released). The event was reported online media in several languages including

major anti-virus companies like Symantec and Kaspersky. The proof of concept and alert to users where released 3 months before the first real attack of MAC OSX Ransomware.
- Published several papers, tasks, and research on Cybersecurity and Multi-Agent Systems.
- Participation as an organizer and IT coordinator in the XVII SIGE (Symposium of Operational Applications in Areas of Defense).

2º/1º Command and Control Group (21GCC), Canoas, Brazil **2009 - 2013**
Brazilian Air Force Squad focused on Command and Control Infrastructure of military operations.

Chief, IT Section Jan. 2009 – Dec. 2013

- Administered all aspects of administrative and operational computer networks including security, maintenance, asset allocation, and logistics, reporting directly to the Squad Commander.
- Conducting a situational awareness program about social engineering and malware that serving as a model for five other squads.
- Development and application of a methodology that seeks to identify the most likely users to be targeted by social engineering attacks that make use of malware as a vector of infection.
- Discovered a critical XSS flaw in the electronic document management system used by the Brazilian Air Force and Army.

Integrated Center of Air Defense and Air Traffic Control (CINDACTA III), Recife, Brazil **2006- 2009**
This Air Traffic Control Center is responsible for overseeing, coordinate and maintain all air traffic in northeastern region of Brazil and the airspace of the Atlantic Ocean.

Chief, Operational IT Aug. 2006 – Dec. 2009

- Experience with implementation and management of critical systems of Airspace Control Department (DECEA).
- Coordinate the parallel operation during the transition from airspace control system developed by THALES ALENIA SPACE Company (MITRA) to the system developed by ATECH foundation (X -4000).
- Responsible for managing the flight plan treatment team in northeastern Brazil.

Chief, Administrative IT Aug. 2006 – Dec. 2009

- Development and coordination of the inoperability equipment control system (HYDRA), which served the entire northeastern region (approximated 2000 users).
- Development of the institutional site.
- Hardware maintenance team management.

Recife Air Force Base (BARF), Recife, Brazil **2003- 2006**
Brazilian Air Force Base with a network that supports approximately 1,200 users.

Chief, IT Section Jan. 2003 – Aug. 2006

- Responsible for creating and implement the Network Security Policy.
- Development of software able to control the hardware inside each computer.
- Several successful investigations about violations of security policy.
- Performed periodic network penetration tests to identify security flaws and vulnerabilities.

Fortaleza Air Force Base (BAFZ), Fortaleza, Brazil **2002- 2003**
1º/5º Aviation Group is a Squad of Fortaleza Air Force Base, with a network that supports approximately 200 users.

Manager, IT Section Mar. 2002 – Dec. 2003

- Management of preventive and corrective computers maintenance.

- Update and monitor network security solutions.
- Development of flight records management system.

EDUCATION

WOLVERHAMPTON CYBER RESEARCH INSTITUTE, Wolverhampton, United Kingdom, 2019
PhD research in progress: Cybersecurity (Advanced Persistent Threat Detection)

BRAZILIAN AIR FORCE INTELLIGENCE CENTER (CIAER), Brasília, Brazil, 2018
Intelligence Analysis Course

AERONAUTICS INSTITUTE OF TECHNOLOGY (ITA), São José dos Campos, Brazil, 2016
MSc in Computer Engineering: Cybersecurity (Advanced Persistent Threat Detection)

BRAZILIAN AIR FORCE UNIVERSITY (UNIFA), Rio de Janeiro, Brazil, 2012
Public Management (MBA)

BRAZILIAN AIR FORCE ACADEMY (AFA), Pirassununga, Brazil, 2001
Bachelor of Aeronautical Sciences / Military Pilot

PROFESSIONAL DEVELOPMENT

Daryus Cybersecurity MBA instructor, Malware Analysis and Reverse Engineering.

Brazilian Army Cyber Warfare Course Instructor, Malware development / detection, Brasília, Brazil, 2018

OWASP LATAM TOUR Leadership, Brasília, Brazil, 2018

2nd Brazilian Cyber Security Summit speaker, **"**Cool, simple and stealthy data exfiltration and C2 channels", São Paulo, Brazil, 2018

Campus Party Brasília speaker, "PDF are safe? Think one more time...", Brasília, Brazil, 2018

1st Brazilian Cyber Security Summit speaker, **"**Detecting rootkits", São Paulo, Brazil, 2017

Campus Party Brasília speaker, "Demystifying ransomware: What is and how to counter this threat?", Brasília, Brazil, 2017

6th Edition of GRC International + 5th Edition DRIDAY Latin America speaker, "Cyber Security - Threats and Challenges. What else is ahead?", São Paulo, Brazil, 2017

SPECTRUM Magazine, Cybersecurity reviewer, ISSN 1981 4291

OWASP 16 Brasília speaker, "MADEC, an immune inspired APT detection architecture", Brasília, Brazil, 2016

DC5561 DEFCON Group speaker, "Simple and effective ransomware evasion techniques", Brasília, Brazil, 2016

Commander stage, Brazilian Air Force, Rio de Janeiro, Brazil, 2015

XVII Symposium of Operational Applications in Areas of Defense, ITA, São José dos Campos, Brazil, 2014

Team Resource Management Course, DECEA, Rio de Janeiro, Brazil, 2009

Information Security Symposium, São José dos Campos, Brazil, 2007