André Tavares

tavares.re/blog | github | linkedin | andretavare5@proton.me

CTI Researcher with CS background, experienced on tracking malware, specifically its campaigns, distribution methods and network infrastructure, through malware analysis, reverse engineering, and threat intelligence. Always looking for new challenges and ready to help the team. I enjoy outdoor activities, playing guitar and casual gaming.

Experience

Senior Threat Researcher 2022 – Present
BitSight - Security Ratings *Remote*

- Malware Research on families such as PrivateLoader, FluBot, IcedID and Gozi, including botnet trackers development, malware analysis and reverse engineering.
- Blog Post — FluBot Persists: Infecting Europe and Australia.

Threat Researcher 2020 – 2021
BitSight - Security Ratings *Remote*

- Malware Research on families such as Trickbot, FritzFrog, Mozi and BazarBackdoor, including botnet trackers development, malware analysis and reverse engineering.
- ML work on domain clustering to filter noise from domain registration tools, using Spark on Amazon EMR.
- Blog Post — Backdoors Pre-Installed on Cheap Android Devices.

Junior Threat Researcher 2018 – 2019
BitSight - Security Ratings *Lisbon, Portugal*

- Classification of botnet C&C domains through OSINT, malware analysis and reverse engineering. Creation of network signatures (Suricata).
- Development of tools (Python) and processes to optimize domain registration and research.
- Blog Post — Fraudulent Ads SDK Installed On 15 Million Android Devices.

Education

M.Sc. in Computer Science and Engineering 2013 - 2017
Instituto Superior Técnico - Universidade de Lisboa *Lisbon, Portugal*

- Specializations: Cyber Security & Software Engineering (Universiteit van Amsterdam).

Skills

Infosec: Malware Analysis, Reverse Engineering, Threat Intelligence
Computer Languages: Python, C, Bash, ASM, PySpark, SQL, JavaScript, Java.
Personal: Curiosity, Persistence, Dedication, Determination, Analytical Thinking, Critical Thinking, Focused, Team Work, Fast Learner, Problem Solving.
Tools: Ghidra, IDA, x64dbg, Yara, VS Code, Git, Docker, Kibana, Apache Spark, Jupyter Notebook, Suricata, JADX.
Languages: Portuguese, English, Spanish.

Courses

Beginner Malware Analysis — Daniel Bunce (Security Joes)
Python Ethical Hacking — Udemy
Apache Spark for Data Engineering and Machine Learning — edX
Machine Learning with Python: Foundations — LinkedIn
A Practical Approach to Malware Analysis and Memory Forensics — Monnappa K A (Cisco)
Tracking an Android botnet by OSINT and APK analysis tools — Suguru Ishimaru (Kaspersky)
Zero 2 Automated: The Advanced Malware Analysis Course — Daniel Bunce and Vitali Kremez (AdvIntel)
Attendance to Botconf 2018-2022 — The Botnet Fighting Conference.

Interests & Hobbies

Infosec, Calisthenics, Play Guitar, Live Concerts, Traveling, Hiking, Casual Gaming, Non-Fiction Books, Sustainability, Minimalism, Volunteering, Plant-Based Diet, Mindfulness, Open-Source Software, Blogging.