

ANDRÉ TAVARES

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

CTI Researcher with CS background, experienced on tracking malware, specifically its network infrastructure, campaigns and distribution methods, 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

Feb 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

Dec 2019 – Jan 2022

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

Jan 2018 – Nov 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

Sep 2012 - Nov 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.

Personal: Curiosity, Persistence, Dedication, Determination, Analytical Thinking, Critical Thinking, Focused, Team Work, Fast Learner, Problem Solving.

Languages: Portuguese, English, Spanish.

Computer Languages: Python, C, Bash, ASM, PySpark, SQL, JavaScript, Java.

Tools: Ghidra, IDA, x64dbg, Yara, VS Code, Git, Docker, Kibana, Apache Spark, Jupyter Notebook, Suricata, JADX.

COURSES, CERTIFICATIONS & CONFERENCES

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.