André Tavares

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

CTI Researcher with CS background, experienced on tracking crimeware malware, including network infrastructure and distribution campaigns, through malware analysis, reverse engineering, and threat intelligence. Always looking for new challenges and ready to help the team.

Experience

Senior Threat Researcher Feb 2022 — Present
BitSight — Security Ratings *Remote*

- Research on malware families such as FluBot, IcedID, Gozi and PrivateLoader, including reverse engineering and botnet trackers development.
- Research blog post: *"FluBot Persists: Infecting Europe and Australia."*

Threat Researcher Dec 2019 — Jan 2022
BitSight — Security Ratings *Remote*

- Research on malware families such as Trickbot, BazarBackdoor, Mozi and FritzFrog, including reverse engineering and botnet trackers development.
- Machine Learning work on domain clustering to filter noise from domain hunting tools, using Spark on Amazon EMR.
- Research blog post: *"Backdoors Pre-Installed on Cheap Android Devices."*

Junior Threat Researcher Jan 2018 — Nov 2019
BitSight — Security Ratings *Lisbon, Portugal*

- Hunting and classification of botnet command and control domains through OSINT, malware analysis and reverse engineering. Writing of network detection signatures (Suricata).
- Development of Python tools to automate domain hunting (selection for registration) & classification.
- 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*

- Specialisations: Cyber Security & Software Engineering (Erasmus @ Universiteit van Amsterdam).

Skills

Languages: Portuguese | English | Spanish
Computer Languages: Python | C | Bash | ASM | PySpark | SQL | JavaScript | Java
Tools: Ghidra | IDA | x64dbg | Yara | VS Code | Git | Docker | Apache Spark | Suricata
Personal: Curiosity | Persistence | Dedication | Team Work | Fast Learner | Problem Solving

Courses, Certifications & Conferences

A Practical Approach to Malware Analysis and Memory Forensics — Monnappa K A (Cisco)
Zero 2 Automated: The Advanced Malware Analysis Course — Daniel Bunce (Security Joes) and Vitali Kremez (AdvIntel)
Machine Learning with Python: Foundations — LinkedIn Learning
Apache Spark for Data Engineering and Machine Learning — edX (IBM)
Attendance to Botconf 2018-2022 — The Botnet Fighting Conference.

Interests & Hobbies

Infosec | Open-Source Software | Blogging | Non-Fiction Books | Calisthenics | Traveling | Play Guitar | Casual Gaming | Sustainability | Volunteering.