Cybersecurity Researcher

Silvia Sebastián

silsebastian.github.io | silvia.sebagon@gmail.com | (+34) 630247313

ABOUT ME

PhD in Cybersecurity with seven years of experience in Attribution, Web Security, and Threat Intelligence. I am a Cybersecurity Researcher who specializes in **building automatic frameworks** for cybersecurity analysts who want to carry out tasks such as **tracking malware** campaigns in mobile markets, **labeling** massive malware datasets, **attributing** domains, or identifying impersonation. By pioneering these automatic frameworks, my fellow malware analysts have experienced significant productivity gains while avoiding manual tedious tasks.

MAIN INTERESTS

- Attribution
- Cyber Intelligence
- Web Security
- Privacy
- Software Development

SKILLS

- Programming Languages (Python, Java, Assembly, SQL, MongoDB, Docker)
- OSINT
- IOC extraction and correlation
- Automating processes
- Natural Language Processing
- Clustering
- Curating and Querying datasets
- Developing research ideas and projects
- Presenting findings
- Documenting and Supporting tools
- Communicating to audiences
- Languages (Spanish-Native, English-C1, French-B2)

EDUCATION AND AWARDS

Ph.D. Software, Systems and Computing
ETSI Informáticos UPM | 2019 - 2023

2018 FPU Grant

Master in Cybersecurity
Universidad Carlos III | 2017 - 2018

Proposed to Best Master Thesis

Bachelor of Computer Engineering
ETSI Informáticos UPM | 2013 - 2017

Best Final Term Project
Grants of Academic Excellence
Honors in 17 Subjects

WORK EXPERIENCE

IMDEA Software Institute | From November 2018
Cybersecurity Researcher

- **Norton Research Group + Eurecom (France)** | Oct. - Dec. 2021
  Predoctoral Stay
- **ETSI Informáticos - UPM** | Sept. 2019 - Aug. 2021
  Teaching Assistance

IMDEA Software Institute | Sept. 2016 - Jun. 2017
Internship in Cybersecurity

OEG - ETSI Informáticos UPM | Apr. 2016 - Sept. 2016
Internship in Ontologies

ACHIEVEMENTS

AVClass

Built a **malware labeling tool** that extracts **tags from malware samples**, enabling rich searches. It is open source and greatly used by the community with more than 500 references and **400 stars on GitHub.**

https://github.com/malicialab/avclass

2020 ACSAC

IOC Searcher

Built a Python tool to **extract indicators of compromise** (IOCs) from artifacts (also known as cyber observables), such as HTML, PDF, and text files. It can identify both defanged (e.g., URL hxxp://example[DOT]com) and unmodified IOCs (e.g., URL http://example.com).

https://github.com/malicialab/iocsearcher

2023 FGCS

2022 JNIC Best Work in Progress

Retriever

Built a cross-platform and cross-market **attribution framework** to **identify** developer accounts in **mobile** markets that belong to the same **operation**. This approach automatically pivots applying OSINT expansions to build an attribution graph that captures the indicators and how they were discovered, preserving the chain of inferences. **Retriever finds more accounts than AV vendors** (that use conventional methods) for 94% of the cases.

2020 ACM SIGSAC CCS **Poster**

WhoseDomain

Built a Python command line tool to **attribute domains and websites**, i.e., to **identify the entity that owns a domain or website**. Given a domain name, if the WHOIS record does not identify a valid owner, then it tries to identify websites hosted on the domain and analyzes their infrastructure and web content to identify the identity of the owner.

https://hub.docker.com/r/dianecode/whosedomain

2023 ACSAC