ANDREA PALMIERI

[email: andpalmier@gmail.com **] . [blog:** andpalmier.com **] . [location: Switzerland]**
[linkedin: /in/andpalmier **] . [github:** andpalmier **]**

PROFESSIONAL EXPERIENCE

Cybercrime Investigations Specialist at **UBS**
Oct. 2022 - ongoing, Zurich (Switzerland)

- Analyze and understand advanced cyber actors, capabilities, and techniques
- Conduct thorough cybercrime and forensic investigations, aiding internal functions
- Collaborate with cross-functional teams to manage and mitigate cyber-fraud cases
- Analyze and respond to threats targeting internal systems and client-facing platforms

Cyber Threat Intelligence Analyst at **UBS**
Jan. 2021 - Sep. 2022, Zurich (Switzerland)

- Monitored, analyzed, and reported on cyber threats to assess organizational risks.
- Evaluated controls, identifying vulnerabilities and recommending effective solutions Produced detailed threat intelligence reports for senior management
- Implemented targeted mitigation strategies based on risk assessments

Information Security Analyst at **PartnerRe**
Oct. 2019 - Dec. 2020, Zurich (Switzerland)

- Conducted security incident detection, response, and investigations
- Strengthened on-premise and cloud security posture
- Conducted vulnerability assessments and recommended improvements

Junior researcher at **SAP**
Mar. 2019 - Sep. 2019, Sophia Antipolis (France)

- Tracked and identified threat actors on web applications, using research tools
- Developed and tested research elements using JavaScript, Python, and JupyterLab
- Collaborated with senior researchers on innovative projects and proposals

Junior researcher at **Fondazione Bruno Kessler**
Mar. 2018 - Oct. 2018, Trento (Italy)

- Created an automated Python tool to assess MQTT instance security
- Executed research on MQTT deployments and conducted state-of-the-art attacks
- Developed and executed sophisticated attacks against MQTT protocol

Junior penetration tester at **Fondazione Bruno Kessler**
Nov. 2017 - Mar. 2018, Trento (Italy)

- Performed comprehensive security assessments of IoT web platforms
- Executed both manual and automated analyses focused on web vulnerabilities
- Delivered findings and recommended effective mitigations

PROJECTS

Security blog at andpalmier.com
Authored posts on malware analysis, machine learning, and phishing. Popular posts:

- Analyzing Android stalkerware
- Malicious document analysis: Emotet distribution
- Flooding phishing kits with fake data

apkingo (66 ★ on GitHub)
GoLang utility designed for extracting detailed static information from APK files.

makephish (44 ★ on GitHub)
GoLang program for cloning and modifying login forms to create phishing pages.

seads (29 ★ on GitHub)
GoLang tool for detecting malvertising on search engines, more info can be found here.

EDUCATION

M.Sc. in Cybersecurity at **EIT Digital**
Sep. 2017 - Sep. 2019, Trento (Italy) and Sophia Antipolis (France)
Summer school on Big Data Analytics at **EIT Digital**
Aug. 2018 - Sep. 2019, Sotckholm (Sweden)
B.Sc. in Computer Science at **Università degli studi di Trento**
Sep. 2013 - Mar. 2017, Trento (Italy)

CERTIFICATIONS

Malware analysis fundamentals
Oct. 2023 | **Pluralsight**
ChatGPT Prompt Engineering for Developers
May 2023 | **DeepLearning.AI**
Operationalising MITRE ATT&CK
Feb. 2023 | **AttackIQ**
Fundations of Purple Teaming
Jan. 2023 | **AttackIQ**
Fundations of Breach & Attack Simulation
Nov. 2022 | **AttackIQ**
Google's Foundations of Project Management
Sep. 2022 | **Coursera**
Google's Data Analytics Specialization
Jun. 2022 | **Coursera**

PUBLICATIONS

Application security through multi-factor fingerprinting

- Patent US20210160277A1
- Presentation at SecWeb 2020

MQTTSA: A Tool for Automatically Assisting the Secure Deployments of MQTT Brokers

- doi: 10.1109/SERVICES.2019.00023
- Publication at 2019 IEEE World Congress on Services (SERVICES)

TECHNICAL SKILLS

Programming Languages: GoLang, Python, and Bash
Analysis: static and dynamic malware analysis, Android reverse engineering, threat hunting, threat intelligence, and data analysis
Additional Tools: Splunk, YARA, and VirusTotal
Cybersecurity Skills: incident response, intrusion detection systems, and vulnerability assessment

LANGUAGES

Italian - *Native speaker*
English - *Fluent*
German - *Basics*