#6 Expert Insights into Advanced Persistent Threats: Analysis, Attribution, and Challenges

Aakanksha Saha, James Mattei, Jorge Blasco, Lorenzo Cavallaro, Daniel Votipka, Martina Lindorfer

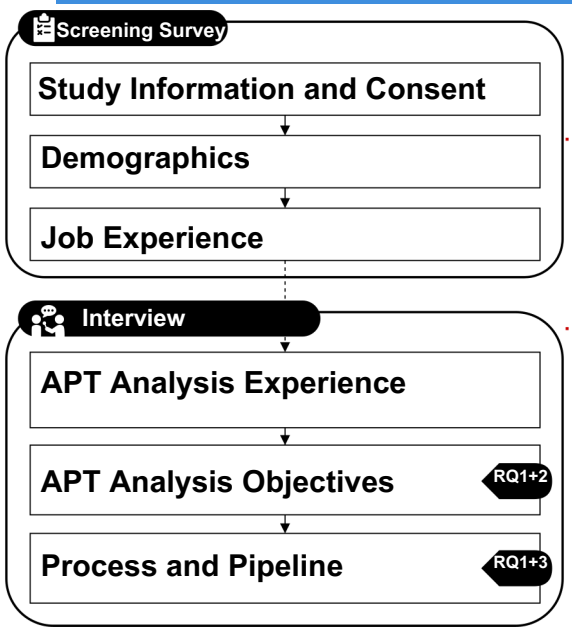
Motivation

- Gain insights into why attribution matters and how it is performed
- Bridge the gap between academic research and real-world practices

Research Questions

RQ1: What are the goals of APT attribution?
RQ2: What is the process of APT attribution?
RQ3: What are the issues in attributing APTs?

Methodology



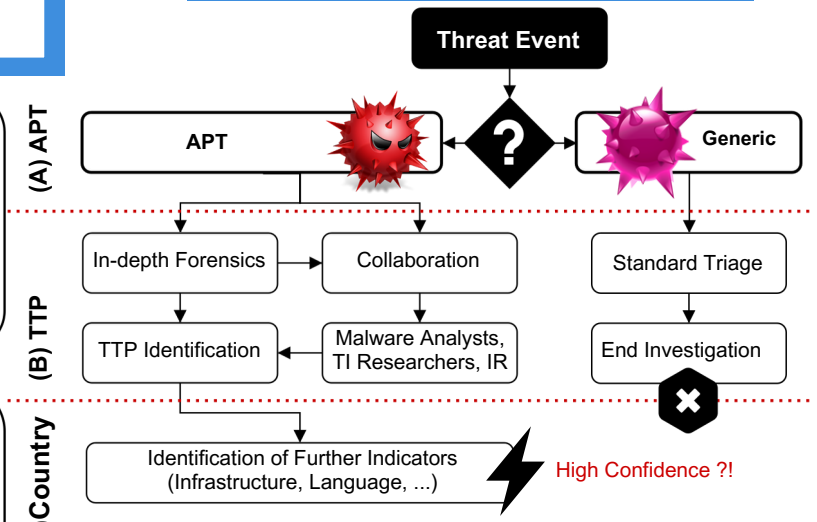
Participants

- ~10 years of experience, primarily from industry (12) and government (2)
- Based in the US and the EU

Goals (RQ1)

- *TTP attribution* informs investigation and effective threat prioritization.
- *Country attribution* helps with long-term remediation and proactive measures.

Decision Tree (RQ2)



Challenges (RQ3)

Tooling Challenges

- Currently minimal automation support in threat data ingestion
- Advanced tools rarely support diverse file formats
- Machine Learning is underutilized in APT event correlation

Process Limitations

- Inconsistent data formats and naming conventions hinder data merging and threat correlation
- Collaboration between entities is difficult and rare

Recommendations

Build Interpretable Attribution System: Connect low-level threat events to tactics, techniques, procedures (TTPs)

Go Beyond Binary Clustering: Expand malware attribution to reflect the diverse, artifact-rich nature of APT campaigns

Focus on TTP Coverage: Shift emphasis from IoCs to more robust and meaningful TTP-based intelligence