UC RIVERSIDE

SOFIA: Finding and Profiling Malware Source-Code in Public Archives at Scale

U. C. Riverside - PI: Michalis Faloutsos
Graduate Researchers: B. Treves, M.R. Masud, O.F. Rokon

Problem:

- We need malware source code for research

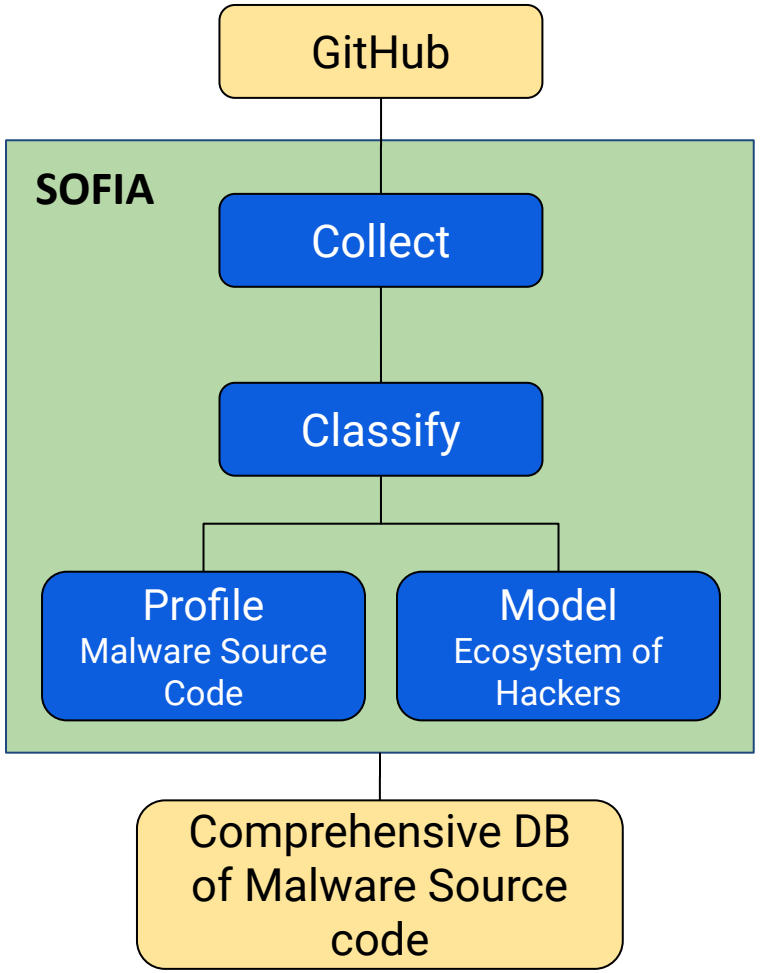
Opportunity:

- There is malware source code on GitHub!

Solution:

Identify malware combining features across three dimensions:

- Metadata
- Code
- Social interactions



Scientific Impact:

- Develop effective methods to identify malware repos
- Develop methods to model the malware ecosystem

Broader Impact and Broader Participation:

- A critical piece towards reducing the $10.5T cost of cybercrime with proactive measures
- Significant commitment to education and BPC

NSF 2132642, UC Riverside,
https://maverics.cs.ucr.edu/sofia/