Hacker Community Collection and Analytics

SBE TTP: Medium: Securing Cyber Space: Understanding the Cyber Attackers and Attacks via Social Media Analytics

Challenge:

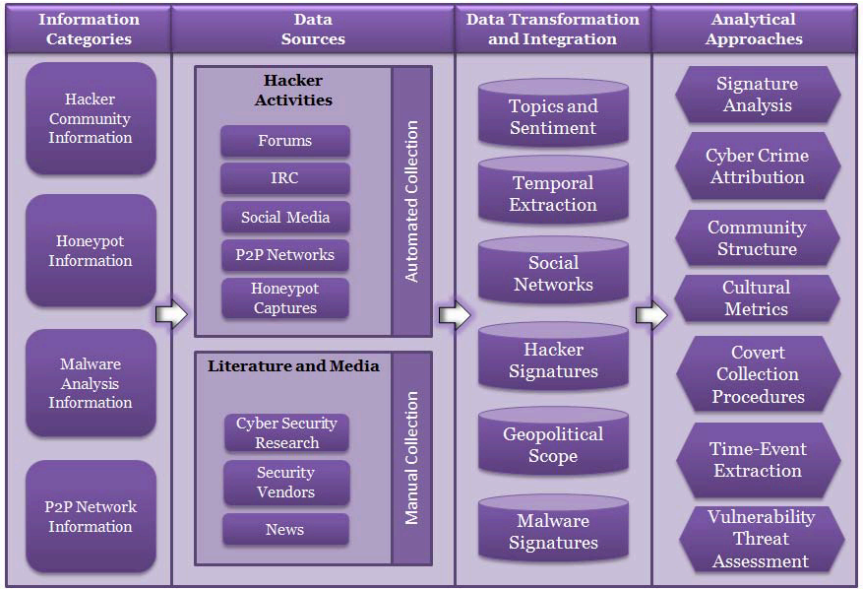
- Developing "methods to model adversaries" is one of the critical but unfulfilled research needs (National Science and Technology Council)
- International virtual hacker communities have spawned across the web to facilitate cyber criminal trade.
- Despite the potential for great societal impact, these communities are understudied.

Scientific Impact:

- A rich, large-scale longitudinal, open source collection of hacker community data for analysis.
  - 3.9M posts (34 hacker forums), 1.5M stolen cards, 21 IRC Channels, 13 Darknet marketplaces
- Automated multilingual content analysis and social media analytics.
  - Identifying: emerging threats, key actors, potential targets, etc.

Solution:

- An integrated and scalable computational social media collection and analytics framework.
- Large-scale collection of forums, IRC, carding shops.
- Multilingual content analysis, social media analytics.



Broader Impact:

- Transitioning research into practice to create a sustainable testbed.
- Aids analysts in understanding the motivation, incentives, dynamics, ecosystems, and trends of hackers.
- Provision of a portal with 16,000 hacker tools.
  - Allows for proactive cyber threat intelligence (CTI).

Project Number – NSF SES-1314631

Principal Investigators:
-Dr. Hsinchun Chen, University of Arizona
-Dr. Salim Hariri, University of Arizona
-Dr. Ron Breiger, University of Arizona
-Dr. Tom Holt, Michigan State University

Management Information Systems
Eller College of Management
The University of Arizona

Artificial Intelligence Lab
Management Information Systems