Hacker Community Collection and Analytics

SBE TTP: Medium: Securing Cyber Space: Understanding the Cyber Attackers and Attacks via Social Media Analytics (NSF SES-1314631)

https://ai.arizona.edu/research/cyber

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

Overview:

- International virtual hacker communities have spawned across the web to facilitate cyber criminal trade.
- Members exchange expertise, malicious snippets of code, or full applications for reputation or financial gain.
- Developing "methods to model adversaries" is one of the critical but unfulfilled research needs recommended in the "Trustworthy Cyberspace" report by the National Science and Technology Council (2011).
- This project aims to develop an **integrated and scalable computational social media collection** and analytics framework for **large-scale hacker community analysis**.

Examples of Hacker Community Contents

Figure 1. Compromised credentials in hacker community for Bayer, Monsanto, and Dow.

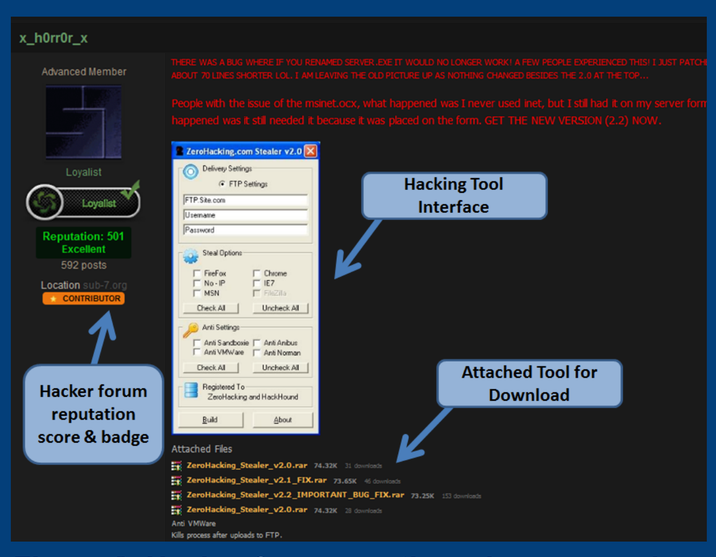

Figure 2. Hacker forum posting where a member shares malicious credential stealing tool.

Figure 3. Dumps of compromised credentials in a hacker forum posting.

Overall Research Framework

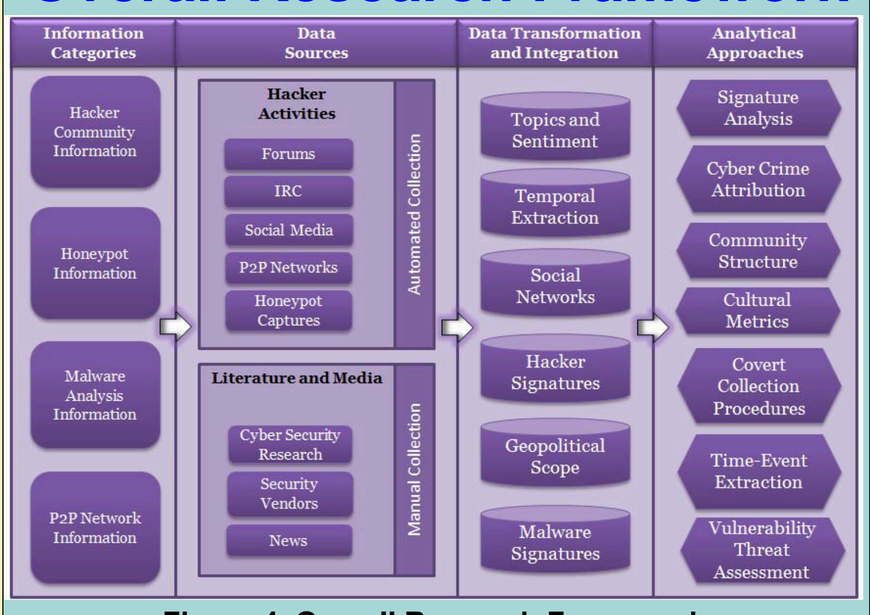

Figure 4. Overall Research Framework

- Our framework utilizes forums, IRC, carding shops to answer critical questions such as:
  - Who are the key community members?
  - What are the key attack vectors?
  - What are the emerging threats?
- We use social network analysis, time-event extraction, classification etc. to aid our analytics

Selected Results: AZSecure Hacker Assets Portal

- Hackers trade thousands of malicious tools on hacker forums (source code, tutorials, and attachments).
- Utilizing scalable web mining and machine learning techniques, we collect 16,000 hacker tools and provide them for educational reuse in a portal format
- Portal allows browsing, downloading, searching, and dynamic analysis of assets.

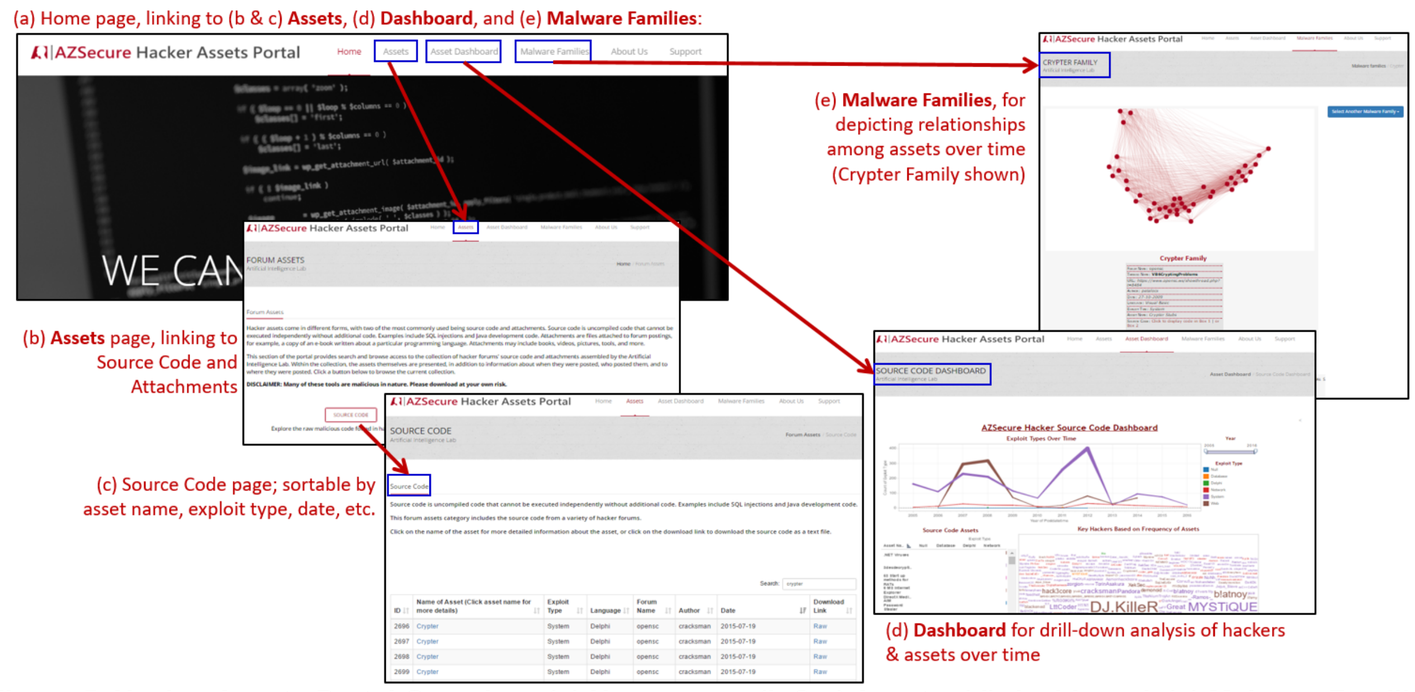

Figure 5. Hacker Assets Portal Overview: (a) Home page, (b & c) Assets, (d) dashboard, (e) Malware Families

Selected Results: Carding Community Collection and Analytics

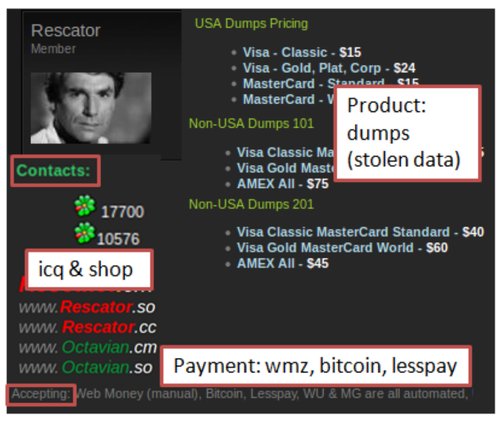

Figure 6. Hackers often share stolen credit cards. Seller information can be found on forums advertisements.

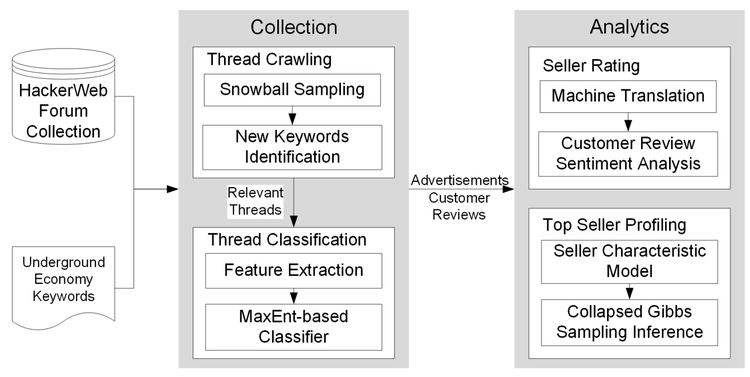

Figure 7. Our AZSecure Text Mining Research System aims to identify the key carding sellers as well as trends of stolen credit cards.

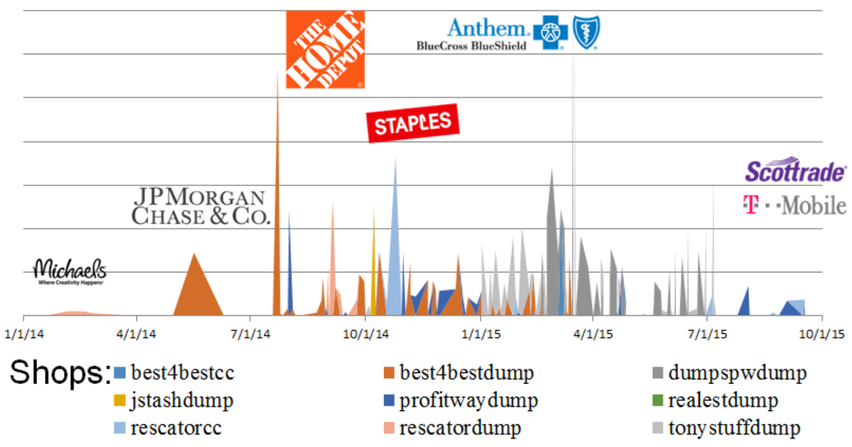

Figure 8. Through our analytic process, we identified the timeline for update patterns of collected carding shops and major leaks

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

Artificial Intelligence Lab
Management Information Systems

Eller College of Management
The University of Arizona