Adventures of a Stolen Credential

Priya Ganguly, Computer Science
Mentor: Dr. Adam Doupé, Associate Professor
CIDSE

Overview

- There are currently an estimated 15 billion compromised credentials that are being sold on underground forums.
- This study gives an insight into what goes on in the underground forums to increase preparedness, response, and recovery.

Research Methods

- Underground forums (RAID and Hack) were analyzed to investigate recent and past activity with credential sharing.
- Different processes of how many types of credentials are shared amongst cybercriminals were identified.
- A clear graph that models the events and potential paths that were studied has been developed.
- A compromised dataset and database descriptions were used to find what kinds of information are being sold and/or shared in the underground forums.
- Interactions between users and subsections of the forums were studied to understand the behavior of users per forum.

Acknowledgements

Adam Doupé
➢ doupe@asu.com

Zhibo Sun
➢ ericsuncs@gmail.com

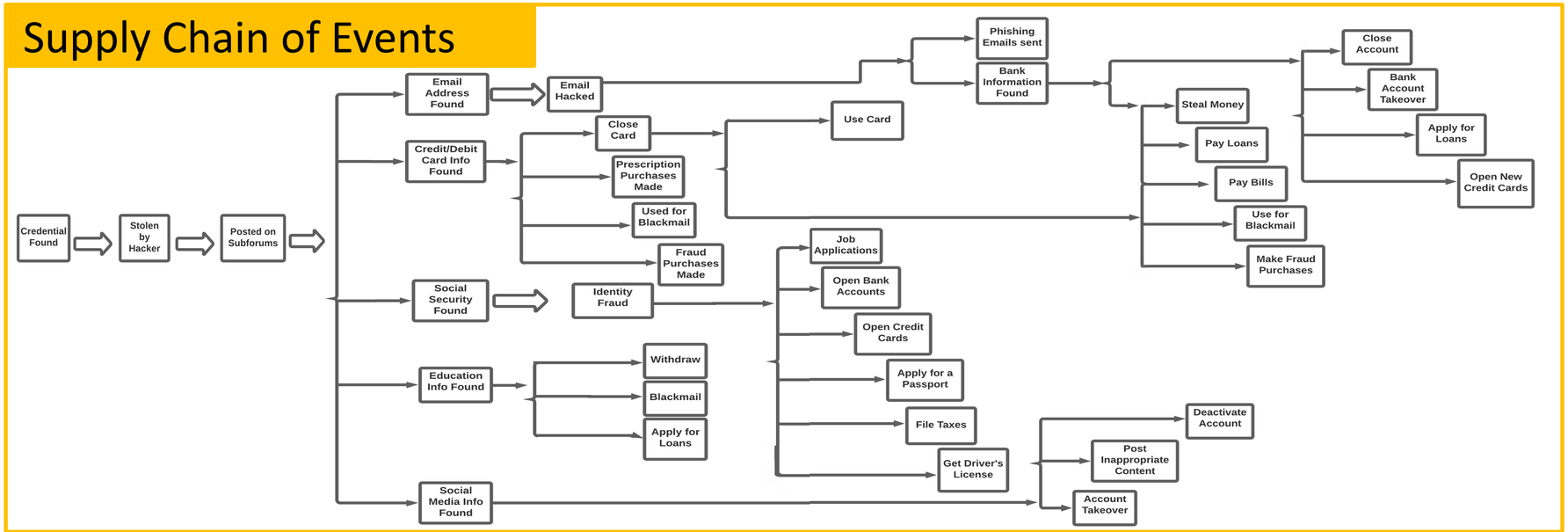
Future Work

- Further investigation on each of the five categories introduced below.
- Analyzing private messages in underground forums.
- Investigating if credentials move from platform-to-platform.

Results

- As seen in the graph to the right, the stolen credentials studied falls primarily into five categories: email, cards, SSN, education, and social media info.
- An overlap between some of the categories is apparent due to the nature of the credential; for example we see that card info can lead to many attacks that bank account information compromises can as well.

Supply Chain of Events



FURI

Ira A. Fulton Schools of Engineering
Arizona State University