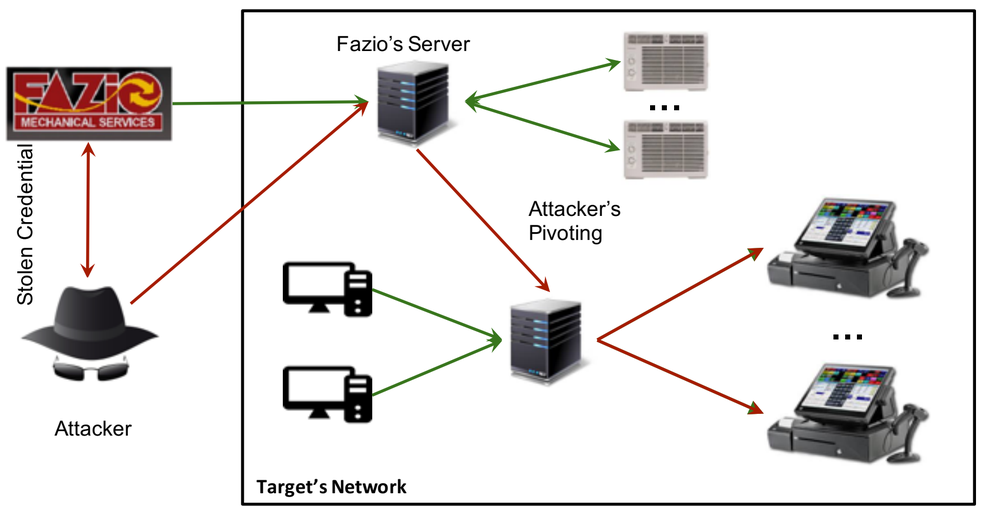
RSAConference Security Scholar

APT-Hunter
Detecting Malicious Logins in Networks

Hossein Siadati -New York University

Problem Statement and Goals

Target's 40 Million Credit Card Breach

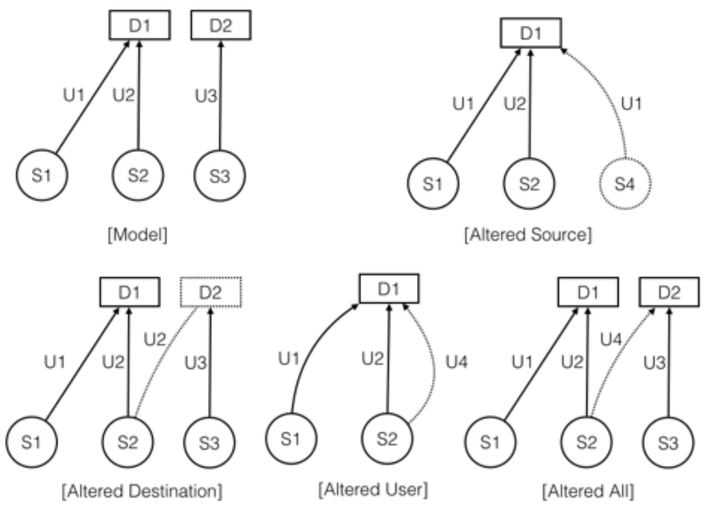


- Attackers use stolen credentials to jump between computers
- Anti-malware, firewall, IDS can not detect this type of jumps
- Number of logins in networks is overwhelming
- There are lots of natural dynamic in network
- **Goal:** Detect malicious logins inside enterprise network

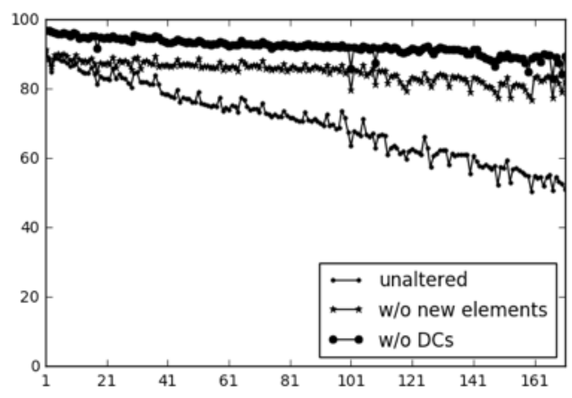
Approach

- Attacker's login creates new links in the graph of logins
- Automatically extract login rules from enterprise network
- Anomaly detection based on deviations from login-rules
- Ranking the abnormal login based on mobility score

Attacker's Jumps



Trend of login changes



Results

- We have developed **"APT-Hunter"**
  - Extract login rules
  - Visualizes the logins
  - Highlights login abnormalities

Evaluation

- Rule extraction is consistent with network configuration
- Logins detected by our system are actually suspicious

Future Work

- Online learning for better ranking of malicious logins