Analysis of Honeypots in detecting Tactics, Techniques, and Procedures changes based on IP Address

Carson Reynolds and Dr. Andy Green

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Introduction

- Financial costs associated with cybercrime have grown from $55 million USD in 2010 to $6.9 billion USD in 2021
- 2019 survey found that 86% of reported breaches were committed by financially motivated actors
- Researchers are studying attacks to learn about threat actor tactics, techniques, and procedures (TTPs)

Research question

Do threat actors change their TTPs based on the geolocation of their target’s IP address?

Literature review domains

- Cybercrime as a Service (CaaS)
- Honeypots in cloud environments
- Cybercrime investigative methods
- Cybercrime policy

Methodology

- T-pot honeypot open-source software used
  - Offers 23 different honeypot options for deployment
  - Contains analysis and data visualization tools
- Identical honeypot instances (hive sensors) deployed in datacenters located in Asia, Australia, Europe, and North America
- Honeypots logged data locally and transmitted data to centralized t-pot instance (hive) containing Elasticsearch, Logstash, and Kibana

Methodology

- Data collected for the month of May 2023
- Intermittent data transmission issues occurred from hive sensors to hive due to level of abuse the hive sensors experienced. All data was safely recorded locally.
- Researchers had to resolve issues of missing data in the hive
  - Created a new hive and manually imported log data from hive sensors
  - Geolocation details had to be recreated manually and verified

Next steps

- Data analysis
- Find the “story”
- Develop recommendations for practitioners
- Submit to A-level journal by the end of the year

Thank you!

- Email – andy.green@kennesaw.edu
- Mastodon – https://infosec.exchange/@AndyGreenPhD
- Website – https://AndyGreen.PhD (slides will be posted here)
- LinkedIn - https://www.linkedin.com/in/andygreenphd

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security