AdaHon: DISTRIBUTED ADAPTIVE HONEYPOT FOR CLASSIFICATION OF ATTACKER PROFILES

LTFE Laboratory for Telecommunications
University of Ljubljana Faculty of Electrical Engineering

GOALS

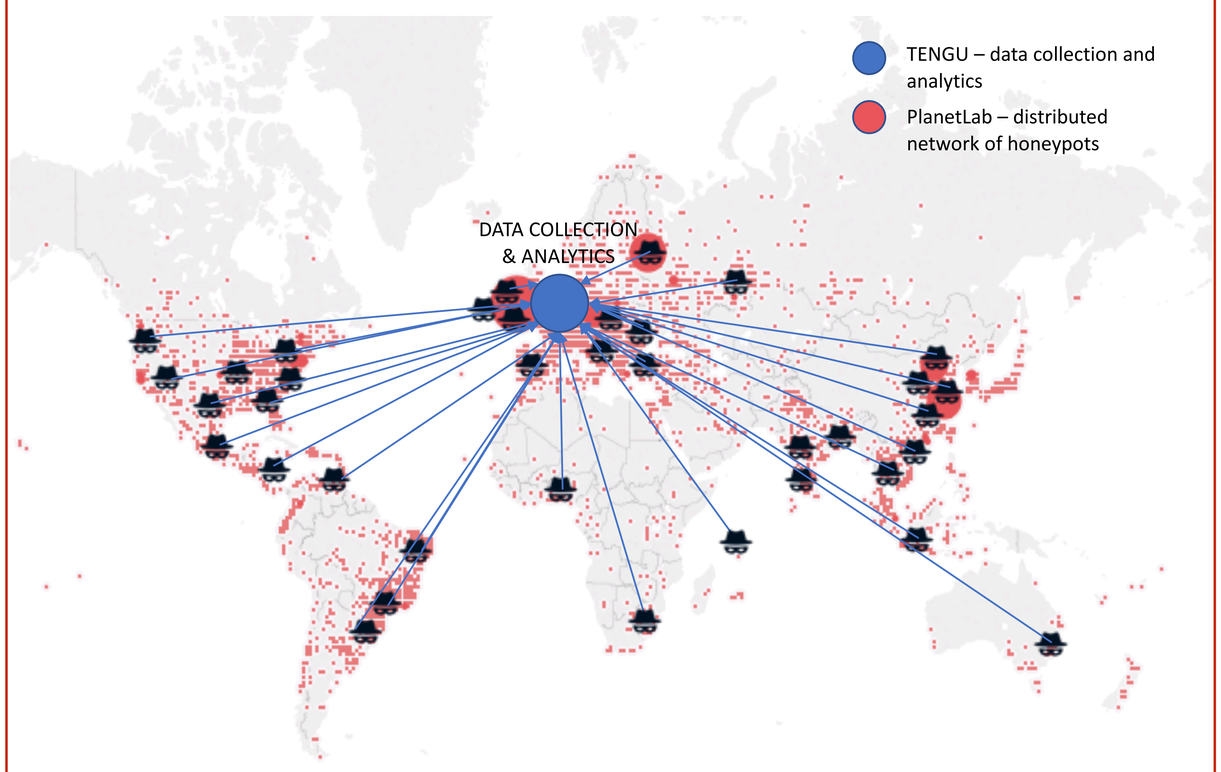
To deploy and validate a distributed network of adaptive honeypots, with the purpose of:

- Gaining comprehensive and up-to-date insights into attacker profiles and modern landscape of hacking tools
- Researching adaptivity of honeypots to delay discovery by attackers and expose most attractive characteristics
- Make the collected data sets available as open data

CHALLENGES

- Design and iteratively validate a large geographically distributed network of honeypots through multiple deployment cycles
- Experiment with different response variations and decoy strategies to improve behavioral capabilities of the honeypots
- Design attacker profiles and cyber-threat reports using big data analytics and interactive visualizations

DEMO SETUP



RESULTS

Deployed high-interaction honeypots on 50+ locations

- Deployment automation and iterative upgrades based on PlanetLab's Kubernetes-based EdgeNet
- Data pipeline based on Logstash and ElasticSearch, using TENGU infrastructure
- Configured Kibana dashboards for high-level analytics

More than 200 GB of raw data, yielding 11 GB of aggregated, pseudonymized and compressed publicly available datasets

Cyberattack landscape and profiling for 2019/2020

- Exploratory analysis and profiling of the attackers and attacks
- Static and interactive visualizations

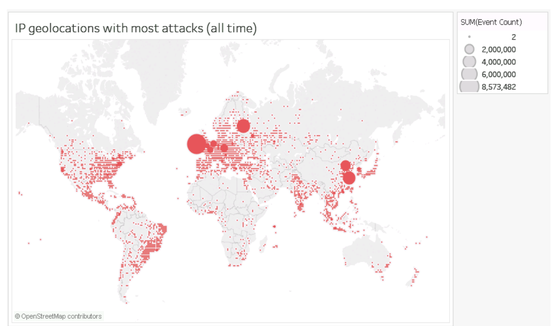
MORE RESULTS

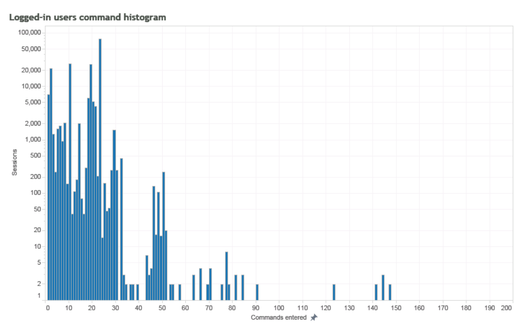
Honeypot interactivity and behavioral adaptation experiments

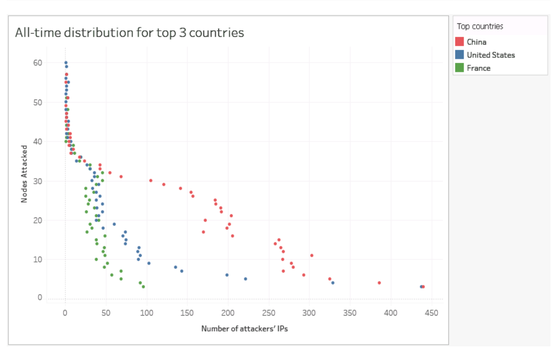
- Experimenting with the effects of reported system parameters (e.g., system resources, hostname) on the attractiveness of the honeypots
- Implementation of a high-interaction honeypot setup (honeypots backed by real Linux containers)

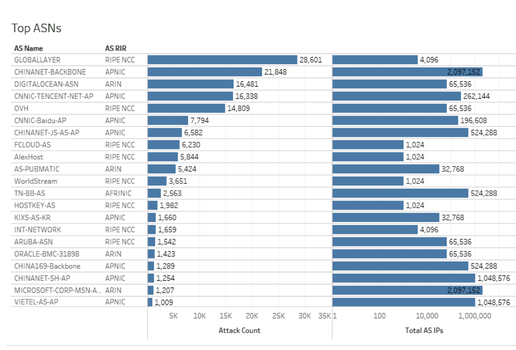
Cyberattack analytics and profiling

- Long-term: attacking centers (source IP, source location, source ASN), classification of most popular attack scripts, malware landscape
- Short-term: real-time attacks detection and characterization, attack depths, sudden events detection









CONCLUSIONS

Significant added value of the experiment

- Scaling of available cybersecurity infrastructure and informing future investments as well as research and business plans
- Extending the scope and depth of cybersecurity know-how
- Publication of open data (DOI: 10.5281/zenodo.3687527)
- Very high value of Fed4FIRE+ testbeds, in particular PlanetLab for deployment of a honeynet on a large number of geographically distributed locations

POST MORTEM

Future plans for infrastructure, partnerships and business

- Scaling of the size, type and geographic distribution of the honeynet and set-up of new research partnerships
- Expanding of the portfolio of cybersecurity projects and experiments, educational courses as well as team members

Future research challenges

- Novel behavior adaptation algorithms using unsupervised learning and high-intensity attack interactions
- IoT and DLT honeypots and cyberattack profiling