A Multi-phased Multi-faceted IoT Honeypot Ecosystem

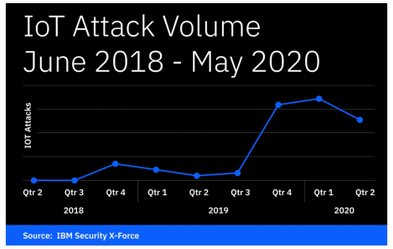
Armin Ziaie Tabari Xinming (Simon) Ou

University of South Florida

Department of Computer Science and Engineering

What are attackers going after on IoT devices?

- IoT devices are growing rapidly and becoming attractive targets
- Understanding the threat landscape early on could help the design and the development



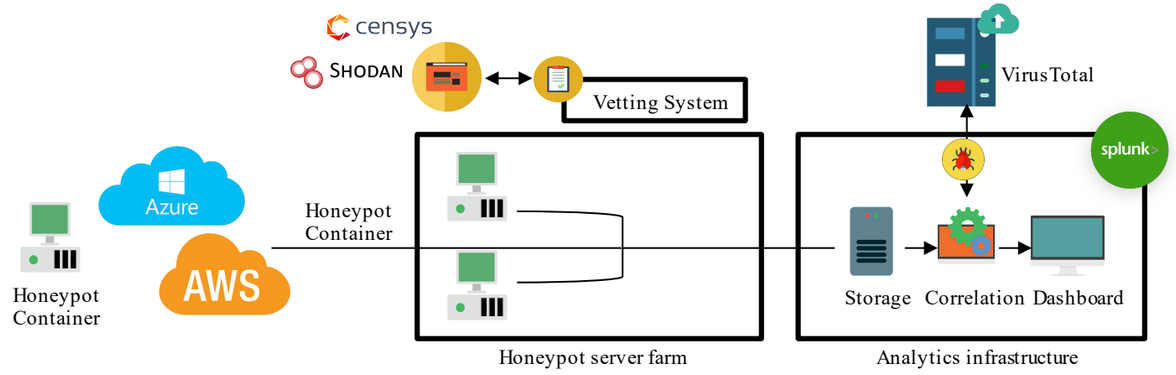
(1) IoT attack volume June 2018 – May 2020

Why not use honeypots to find out?

IOT HONEYPOT CHALLENGES

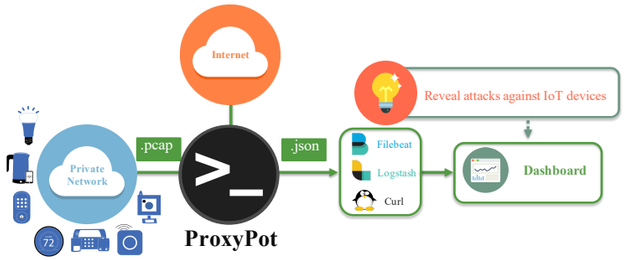
- Large variety of device types
- Physical-connectedness nature and richness of the responses

Our approach: Multi-phased Multi-faceted IoT Honeypot Ecosystem



(1) https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/

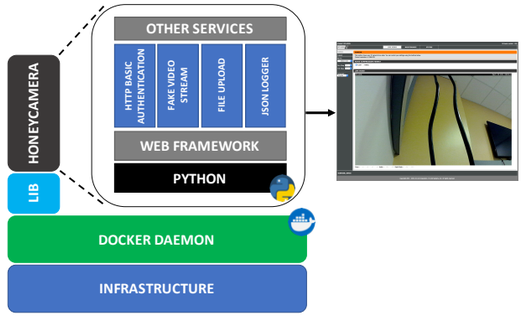
PROXYPOT



A proxy instance that sits between an IoT device and the network gateway and captures all traffic that goes between.

We used the ProxyPot data to create **HoneyCamera**.

HONEYCAMERA



To capture attacks on specific IoT devices, we build a honeypot for **IoT camera** and coined it **HoneyCamera**.

Honeycamera is a low-interaction honeypot for D-Link IoT cameras.

Main Findings So Far

We deployed honeypots for **more than two years**:

- Our preliminary results showed that we were able to attract increasingly sophisticated attack data in each new phase
- Our approach seems to be uniquely capable of capturing human attack activities, as opposed to simply automated attack scripts.

Interesting Cases

Based on our logs we captured **multiple two-step attacks** in our HoneyCamera:

- Attackers exploited a well-known vulnerability that we planted inside the HoneyCamera, to read username and password of the camera
- Then, the same attacking IP logged in through the Camera login page using the stolen credential.

More detailed cases can be found in https://arxiv.org/abs/2003.01218