Ludus project:

Make honeypots great again!

Kalin Ivanov & Ondřej Lukáš

FACULTY
OF ELECTRICAL
ENGINEERING
CTU IN PRAGUE

www.stratosphereips.org/ludus

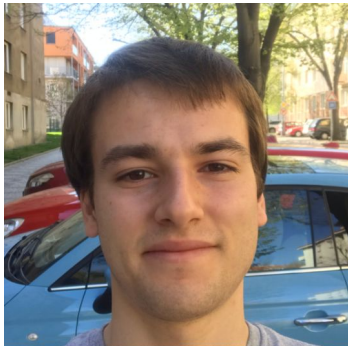
Stratosphere Lab

- Cybersecurity Part of AIC
- https://www.stratosphereips.org/

  @StratosphereIPS

  @StratoLudus
- ludus@aic.fel.cvut.cz - Official Ludus contact
- www.stratosphereips.org/ludus

@ondrej_lukas



@RealKalin

Plan

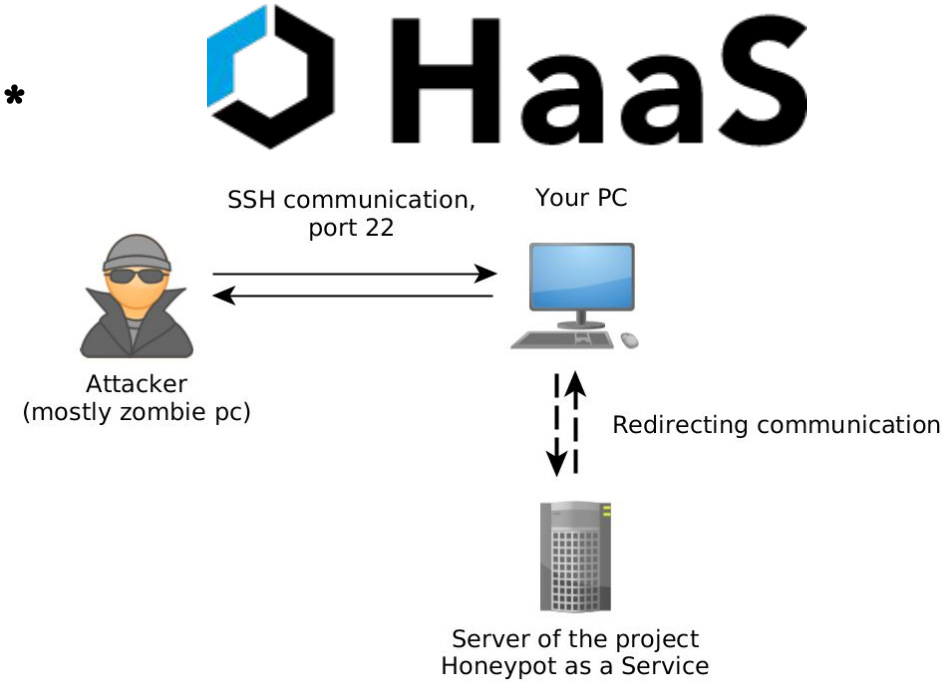
- Why Ludus?
- Defense as a game
- Collaborative defense
- External Security Metric
- Ludus tool

Motivation and Goals of Ludus

- Collaboration with  and TAČR
- Model attackers´ behaviour and use it to create better defense
- Protect users against attacks from the Internet
- Design External Metrics to capture the Security level of devices

Honeypots in Ludus

- TARPIT - iptables module
- Honeypot as a Service*
- Minipot (Telnet)
- Extendable!



* More infotion at https://haas.nic.cz/

Troubles with Honeypots

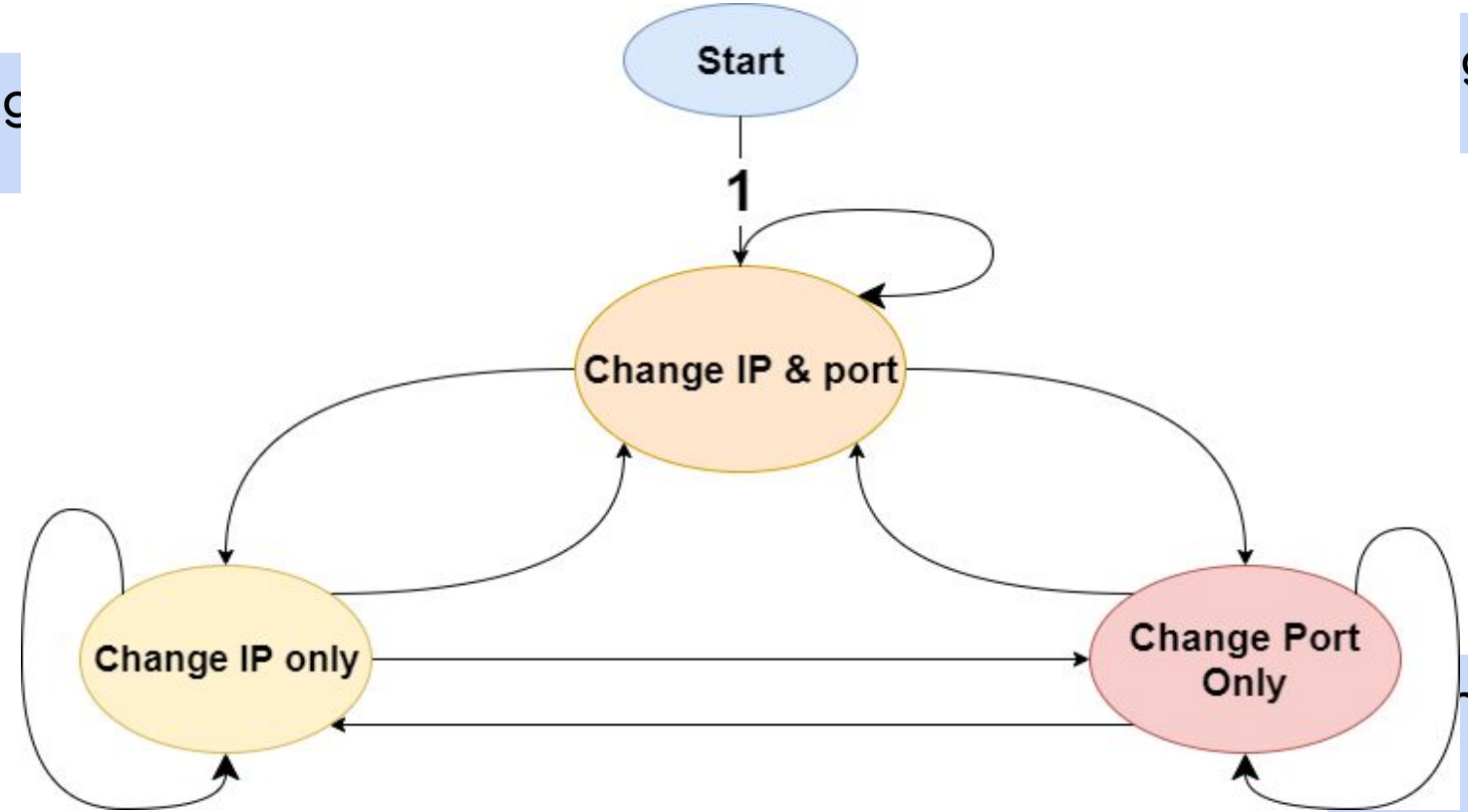
- Where to put them?!
- Static and predictable
- How to use the data?
- Bringing your device in the spotlight?!

Troubles with Honeypots

- Where to put them?!
- Static and predictable
- How to use the data?
- ~~Bringing your device in the spotlight?!~~

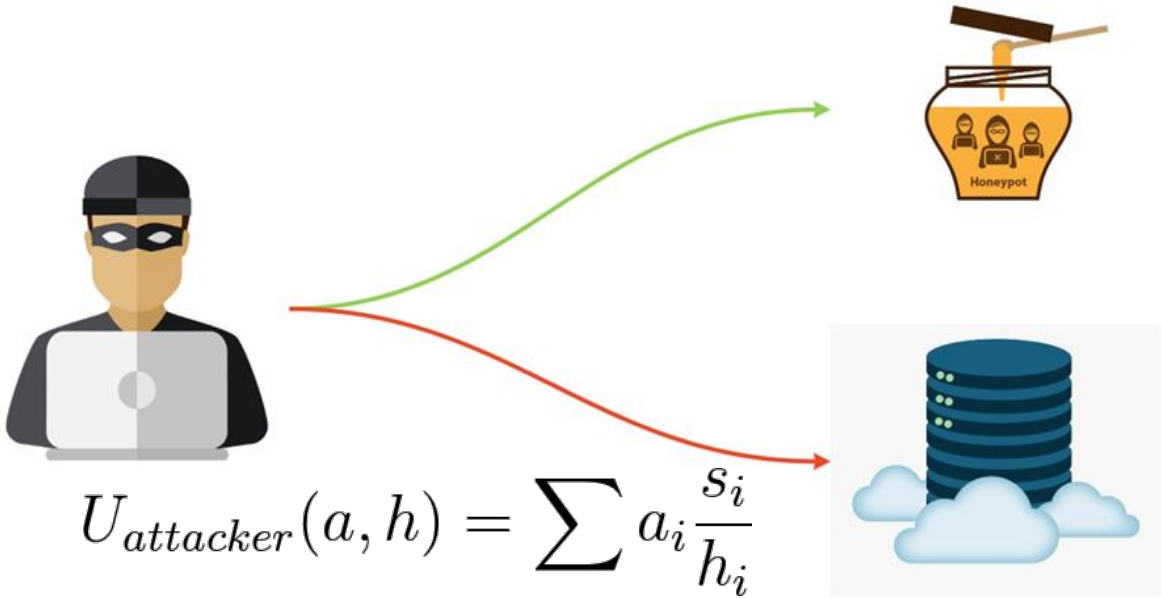
Modeling attacks as a game

Model of Attackers' behaviour



Game-Theoretical Approach

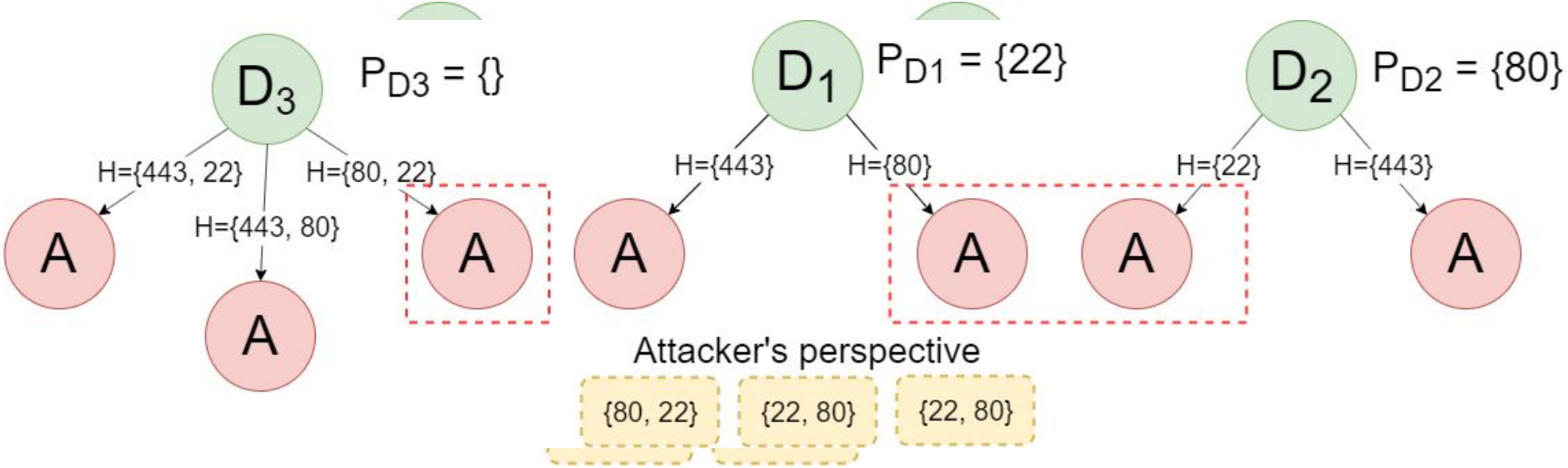
- Model attacks as a game
- Find the optimal strategy
- Minimize attacker's utility
- Save resources



$$U_{attacker}(a,h) = \sum a_i \frac{s_i}{h_i}$$

Joining Forces with Others

- Information Sets ⇒ less information for ⇒ lower utility
- Constraints in number of honeypots



You can’t manage what you can’t measure

Data

2 Types:

1. Packet metadata
2. Suricata alert data

#	pkts_toclient	0
#	pkts_toserver	1
t	protcol	tcp
#	sport	65,204
💻	src_ip	181.174.164.192
t	state	new
t	status	honeypot

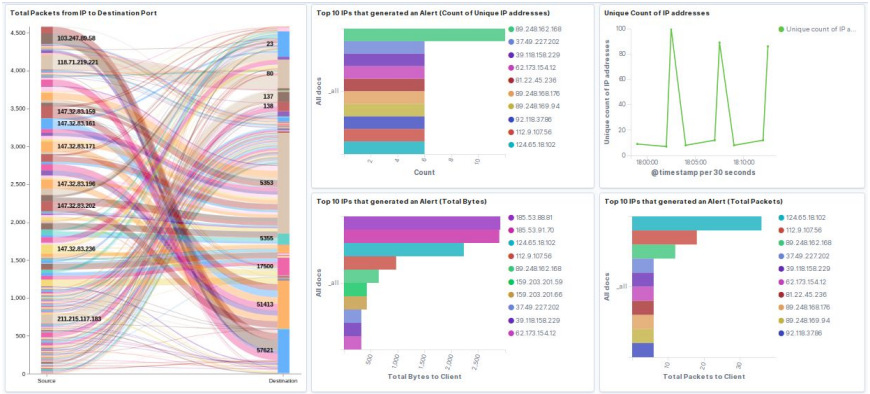
Suricata signatures

1| Not Suspicious Traffic
2| Unknown Traffic
3| Potentially Bad Traffic
4| Attempted Information Leak
5| Information Leak
6| Large Scale Information Leak
7| Attempted Denial of Service
8| Denial of Service

Dashboards

Local dashboard for each user

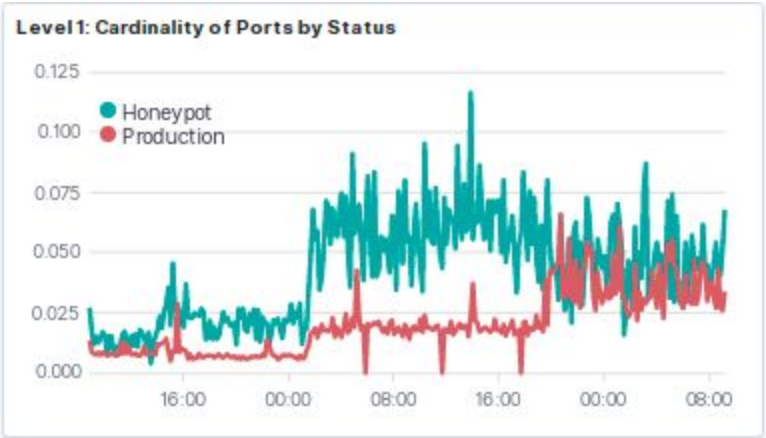
Publicly AAA Data
(Anonymized, Aggregated, Available)

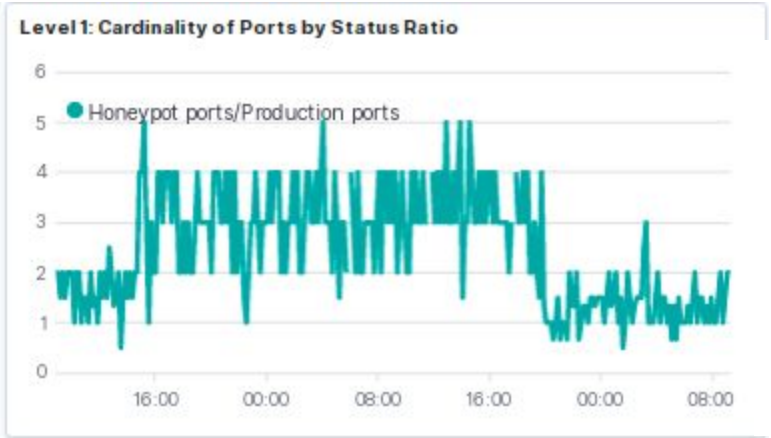


Check out the public Kibana visualizations:

Metrics

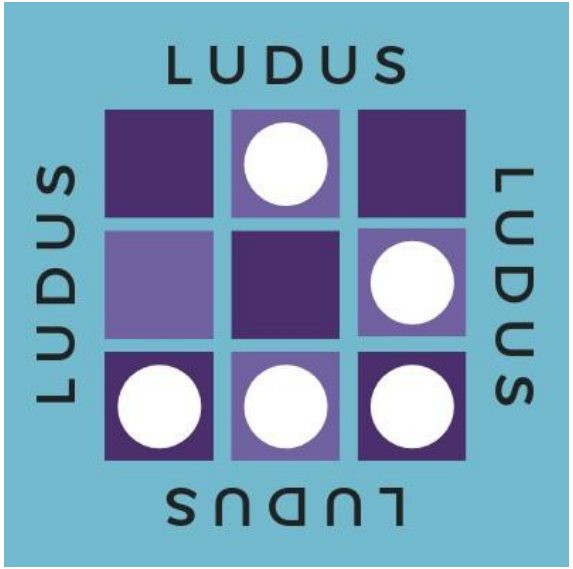
- Overall Security
- Honeypots/Production Ports
- Entropy of attack





Ludus tool

- fully automated
- adapts and updates strategies
- anonymizes and visualizes data
- turris package: ludus



https://doc.turris.cz/doc/cs/howto/installation

https://github.com/stratosphereips/Ludus

Q&A

Thanks for your attention!

@ondrej_lukas
lukasond@fel.cvut.cz

@RealKalin
ivanokal@fel.cvut.cz

https://www.stratosphereips.org/ludus