Project Ludus:

Advanced security tool for your router

Kalin Ivanov & Ondřej Lukáš

Internet a Technologie 19

FACULTY
OF ELECTRICAL
ENGINEERING
CTU IN PRAGUE

www.stratosphereips.org/ludus

Plan

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

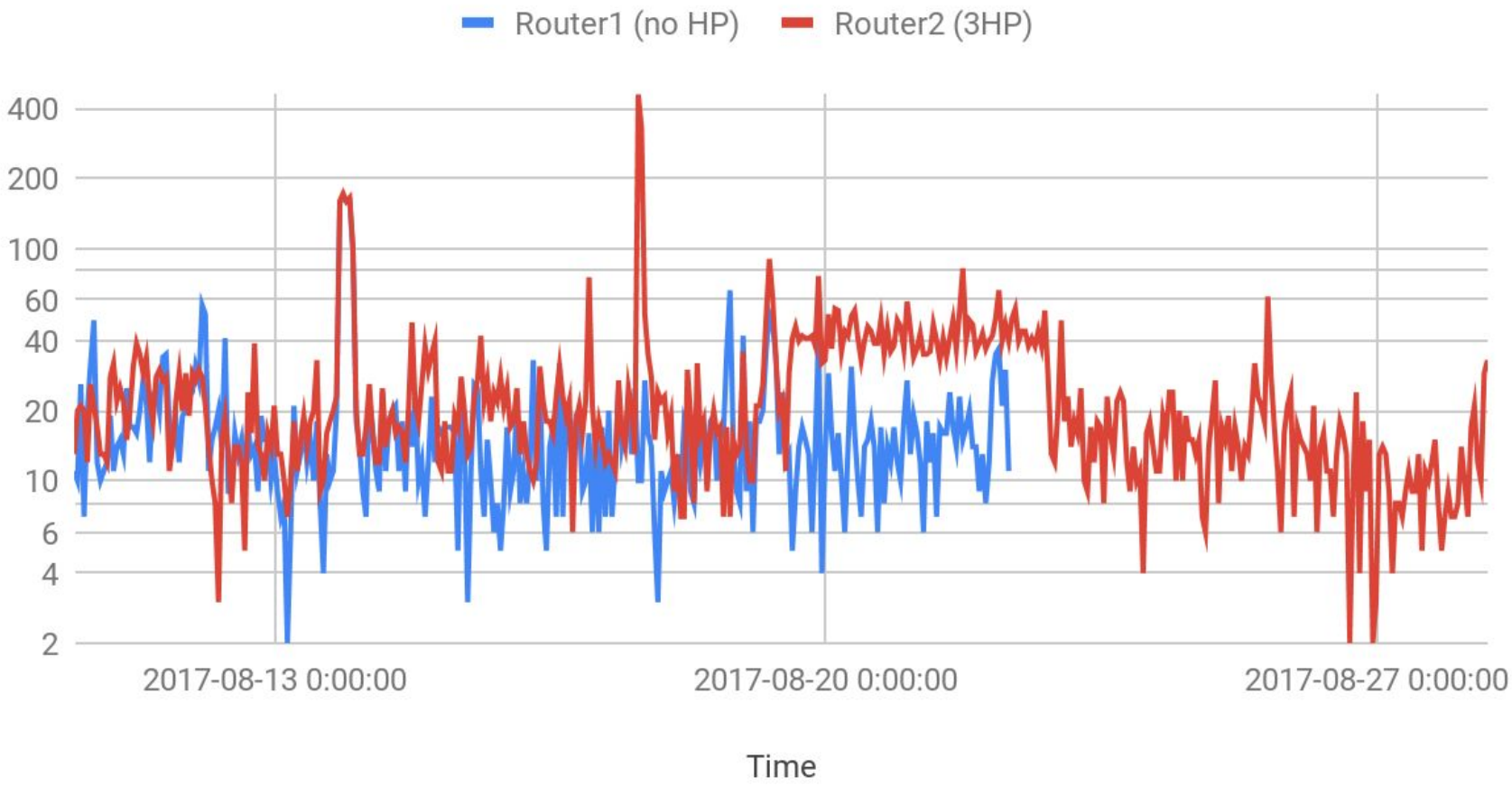
Motivation and Goals of Ludus

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

Troubles with Honeypots

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

Influence of honeypots on the real services visibility



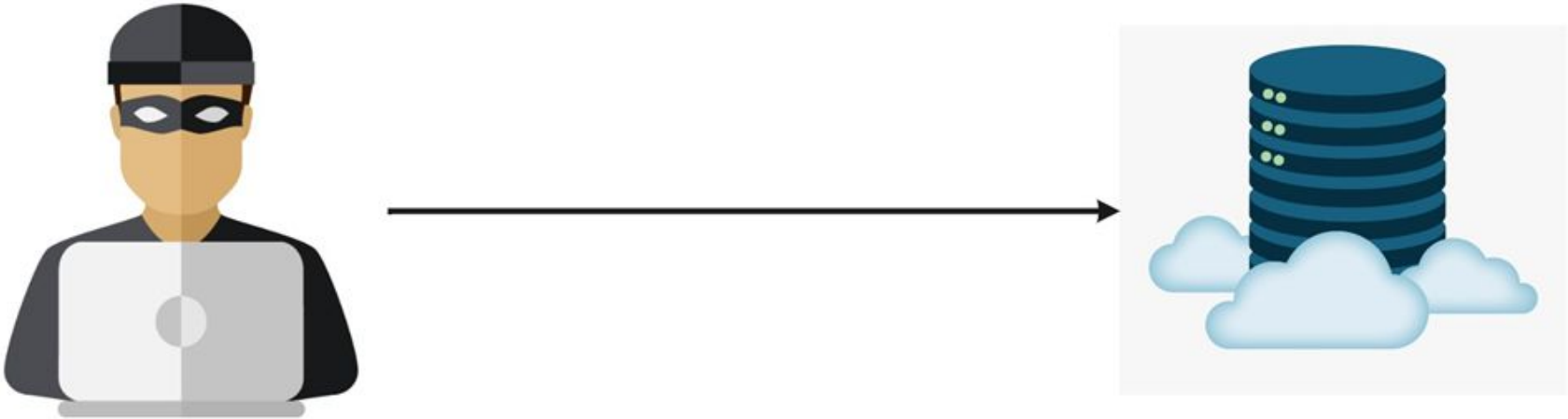
Troubles with Honeypots

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

Do you want to play a game?

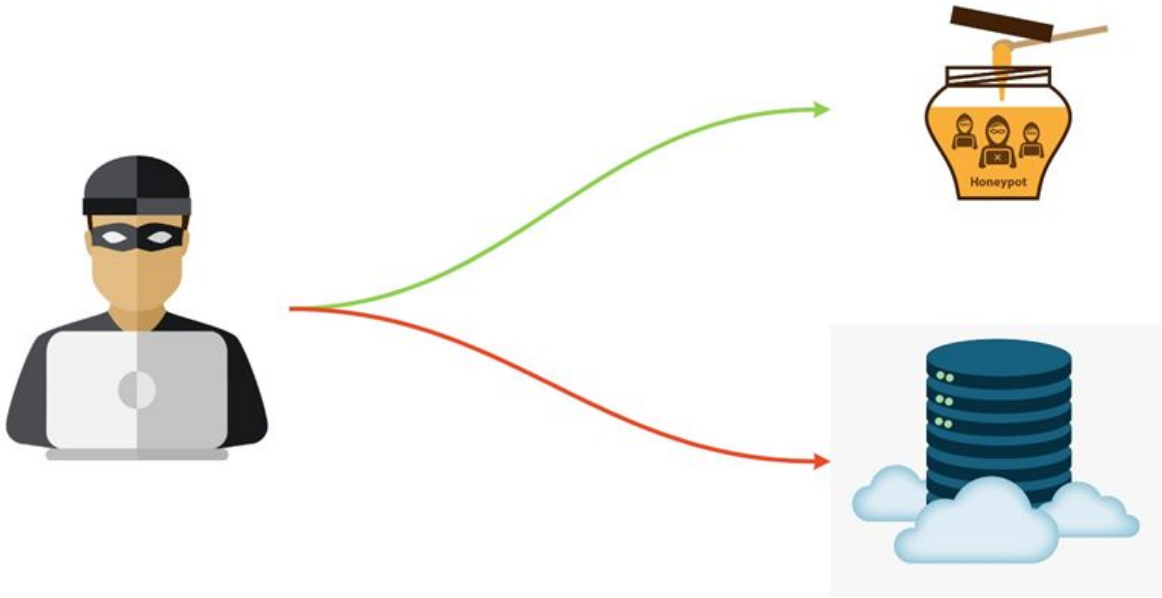
Game-Theoretical Approach

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



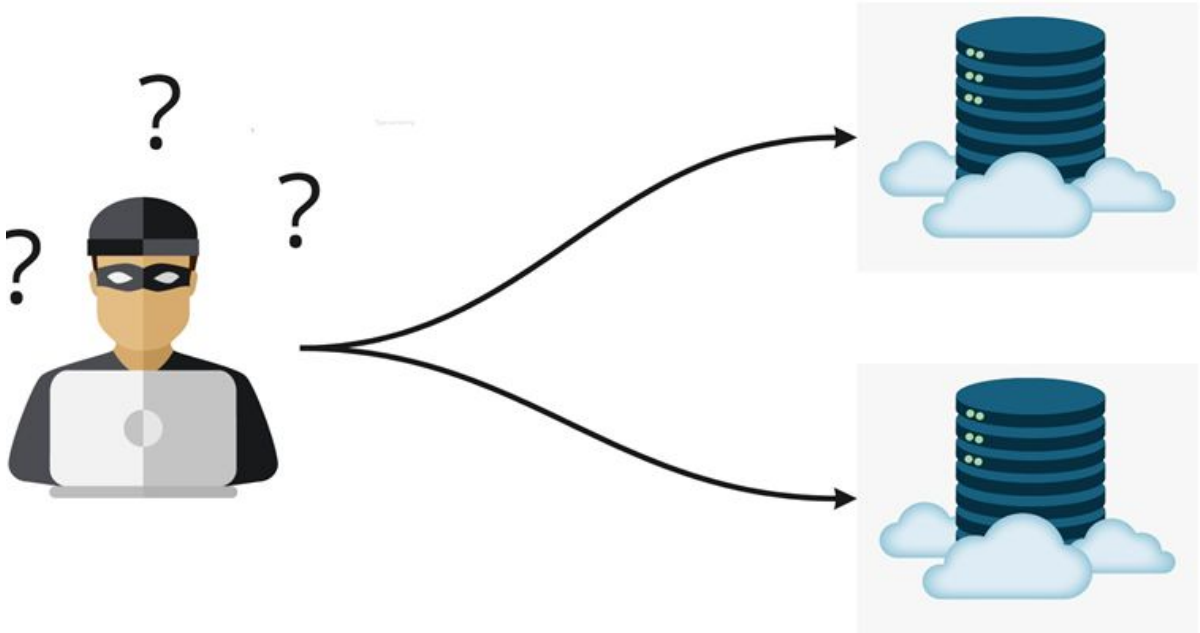
Game-Theoretical Approach

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



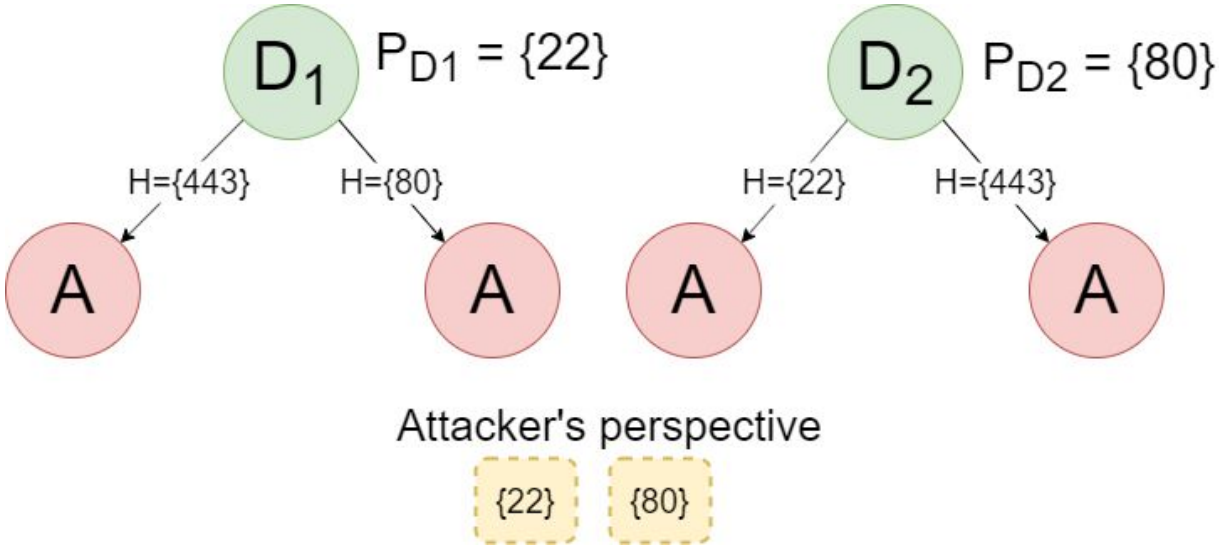
Game-Theoretical Approach

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



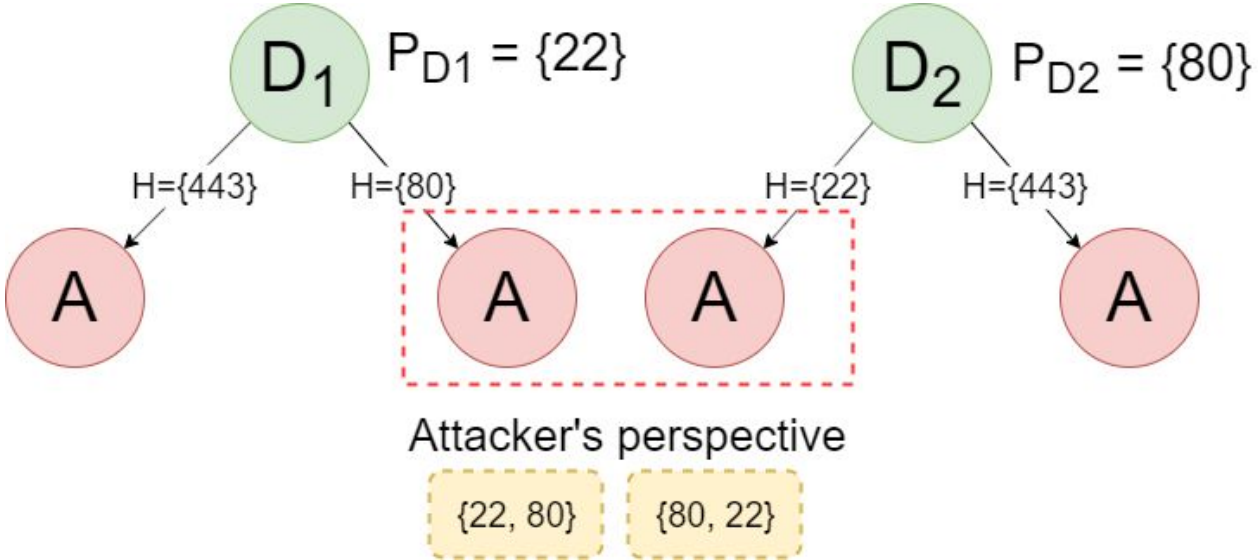
Joining Forces with Others

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



Joining Forces with Others

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



You can’t manage what you can’t measure

Data

2 Sources:

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

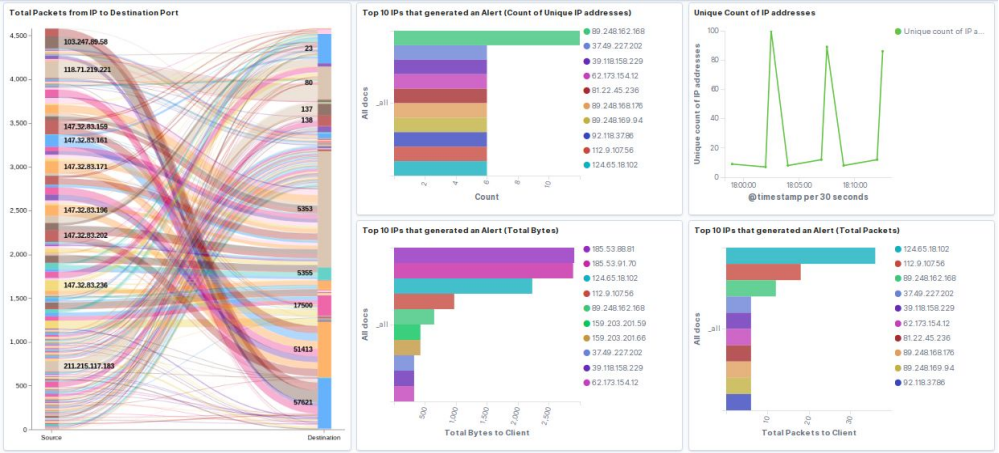
Suricata signatures

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

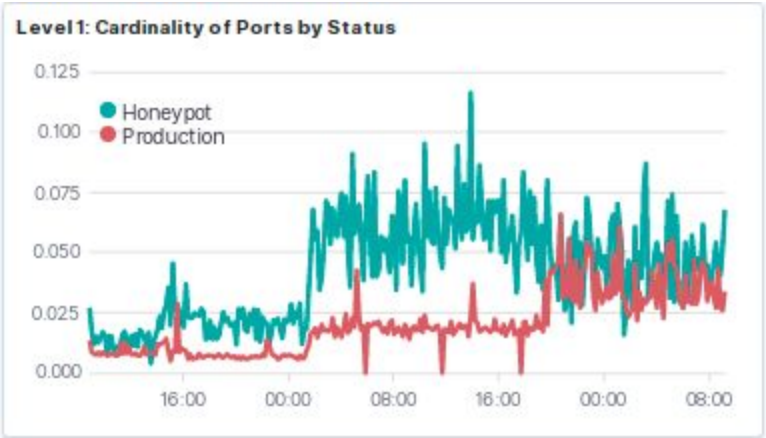
Publicly AAA Data
(Anonymized, Aggregated, Available)

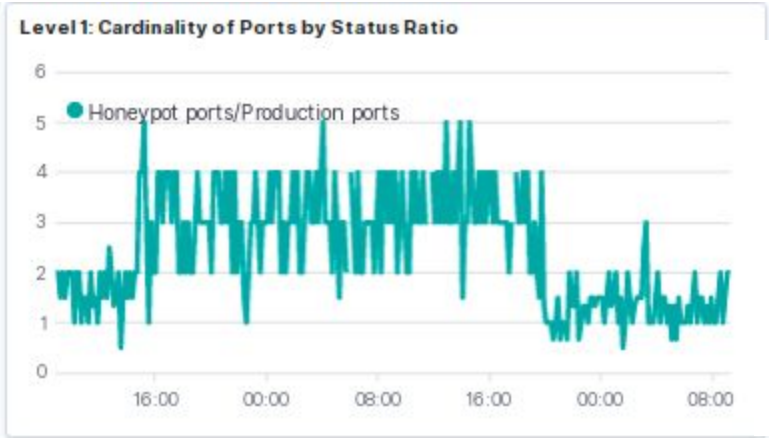


Check out the public Kibana visualizations:

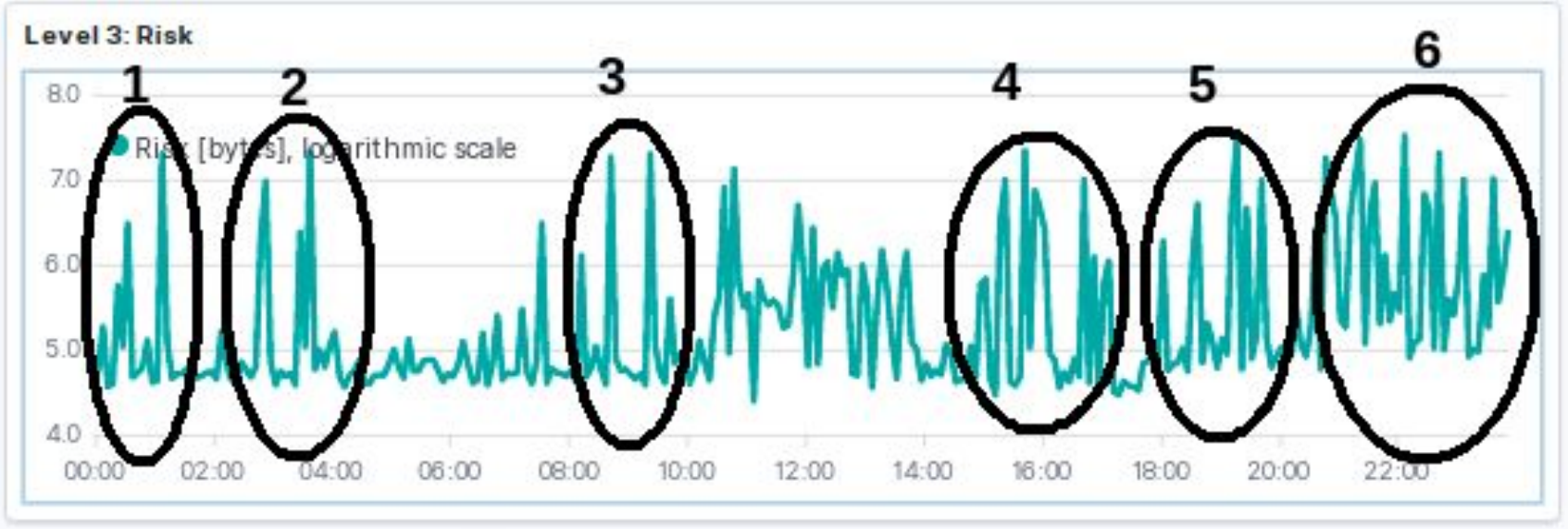
Metrics

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

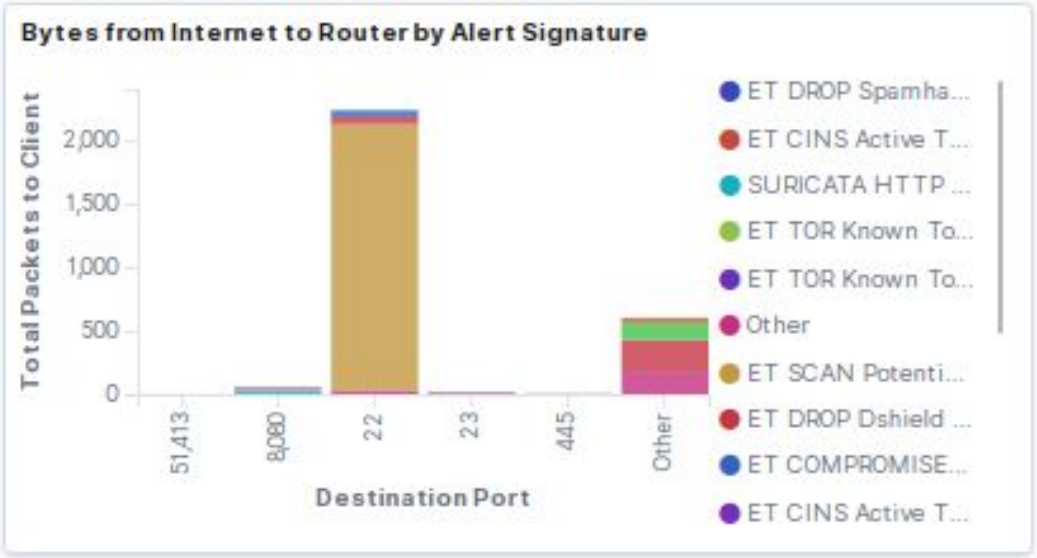


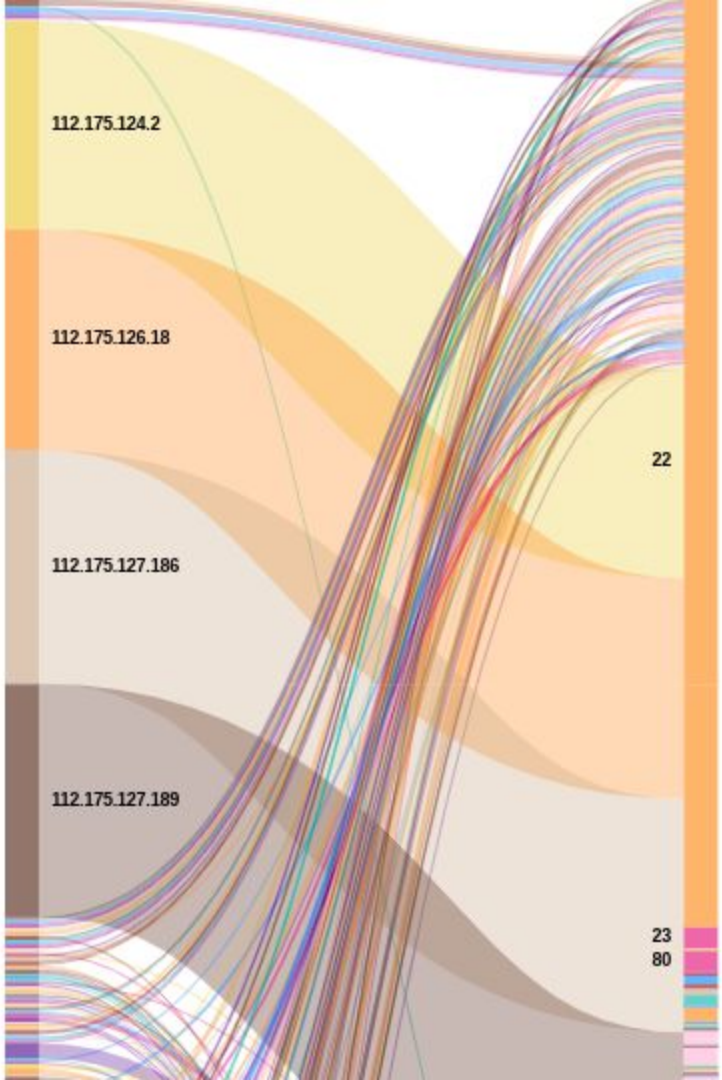


Example

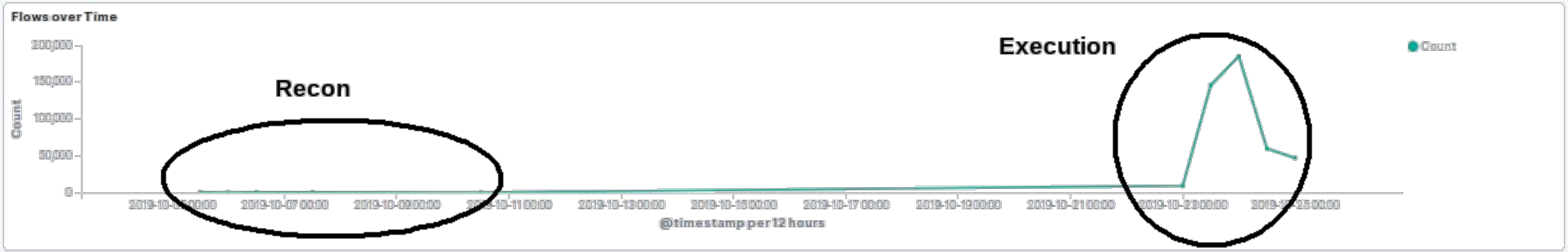

Level 3: Risk
1
2
3
4
5
6
8.0
7.0
6.0
5.0
4.0
Risk [bytes], logarithmic scale
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00

Example


Bytes from Internet to Router by Alert Signature
Total Packets to Client
2,000
1,500
1,000
500
0
51,413
8,080
22
23
445
Other
Destination Port
ET DROP Spamha...
ET CINS Active T...
SURICATA HTTP ...
ET TOR Known To...
ET TOR Known To...
Other
ET SCAN Potenti...
ET DROP Dshield ...
ET COMPROMISE...
ET CINS Active T...


112.175.124.2
112.175.126.18
112.175.127.186
112.175.127.189
22
23
80

Example



209.239.90.114
Emerging Markets Communications de Argentina S.R.L
Added on 2019-10-23 22:12:54 GMT
United States

```
System administrator is connecting from 112.175.124.2

Reject the connection request !!!
```

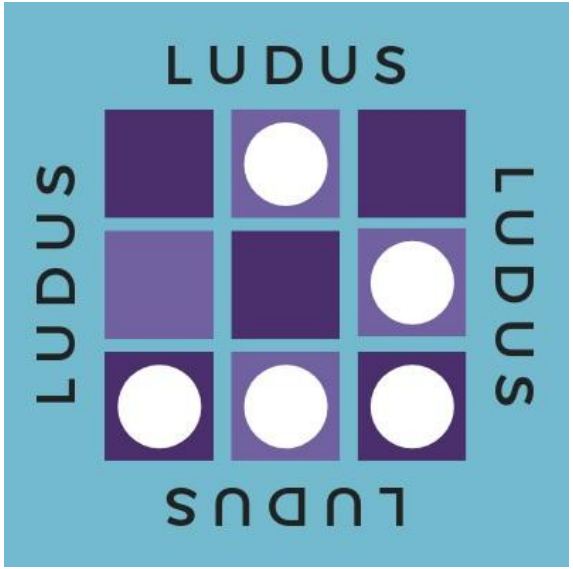
95.210.229.87
95-210-229-87.ip.skylogicnet.com
Skylogic S.p.A.
Added on 2019-10-24 21:52:40 GMT
United Kingdom, Fulham

```
System administrator is connecting from 112.175.124.2,
Reject the connection request !!!
```

https://www.shodan.io/

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