Conferenza GARR 2021
sostenibile digitale

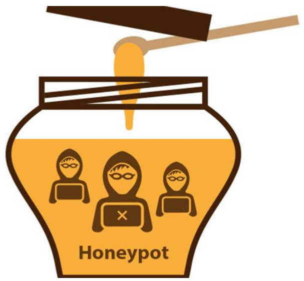
Analysis of Anomalous Traffic Through DPI-Enhanced Honeypots

Tommaso Rescio*, Francesca Soro*,Marco Mellia*, Idilio Drago**
SmartData@PoliTO, *Politecnico di Torino, **Università di Torino

POLITECNICO DI TORINO
SmartData@PoliTO
SmartData

Background

- **Network monitoring for cyber-security purposes;**
- **Darknets** are defined as sets of IP addresses that are advertised without answering any traffic;
  - **Passive traffic only;** ☹



- **Honeypots** are intentionally vulnerable hosts used as decoy for attackers in order to record their malicious activities;
  - **Active engagement of possible attacker;** ☺
  - **Protocol-specific;** ☹
  - **No flexibility.**

Objective

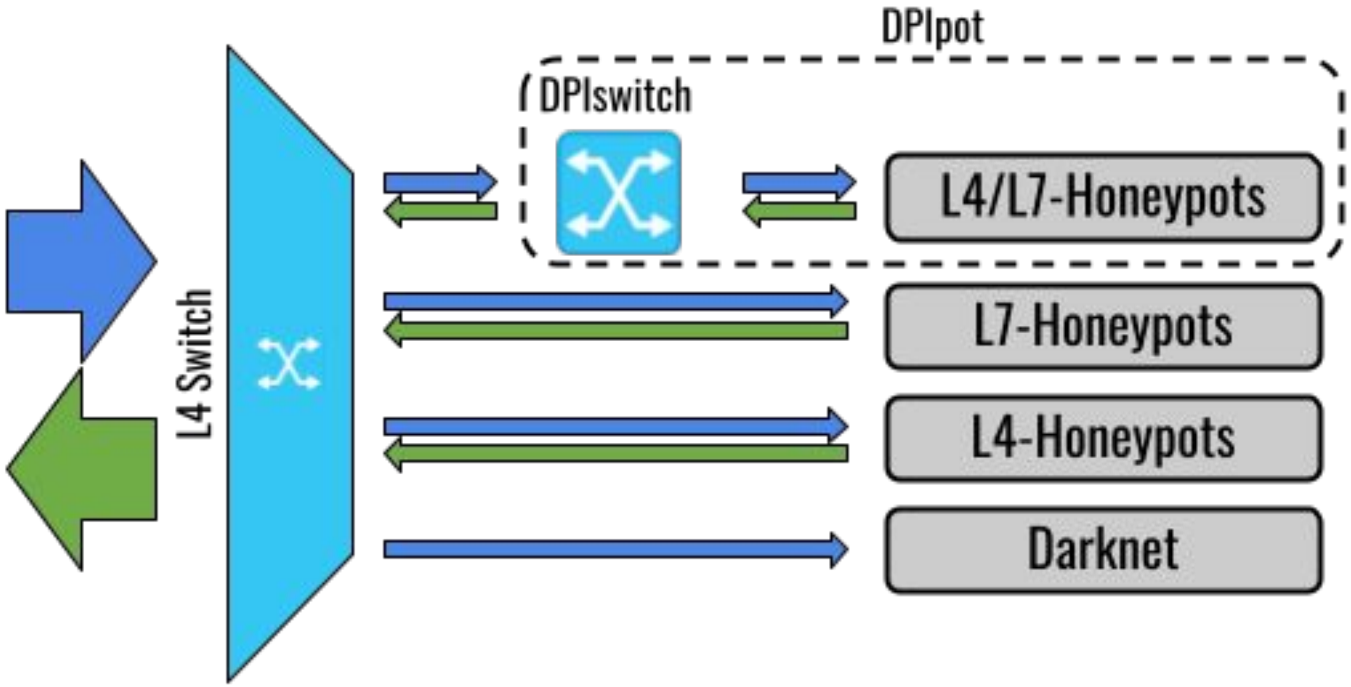
- Engineering of a **novel solution of honeypot**: *DPIpot*
    - Smart and efficient classification of the application protocol by means of **Deep Packet Inspection** (DPI)

- To check whether we can gather **more information** with *DPIPot* than with traditional systems

- Comparing with traditional **Darknet**, **L4-Honeypots**, **L7-Honeypots**

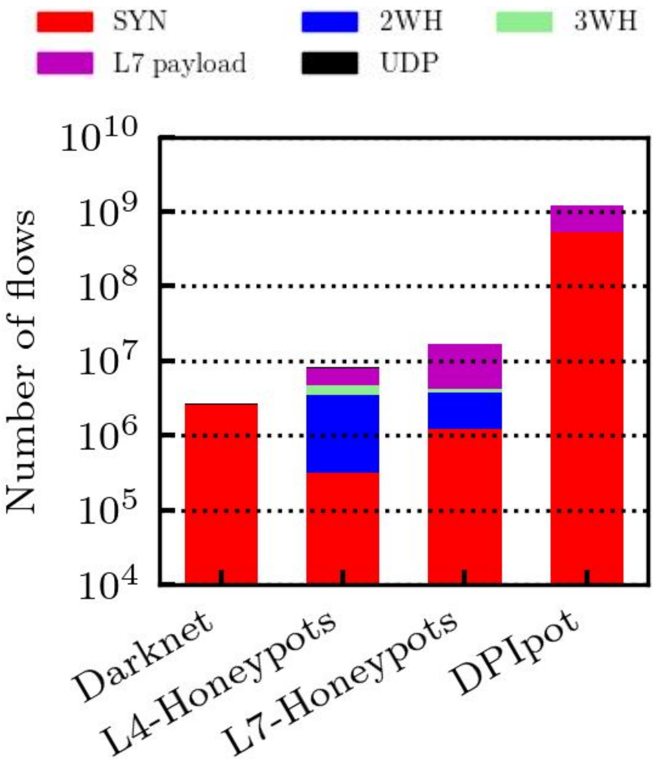
Architecture and Deployment

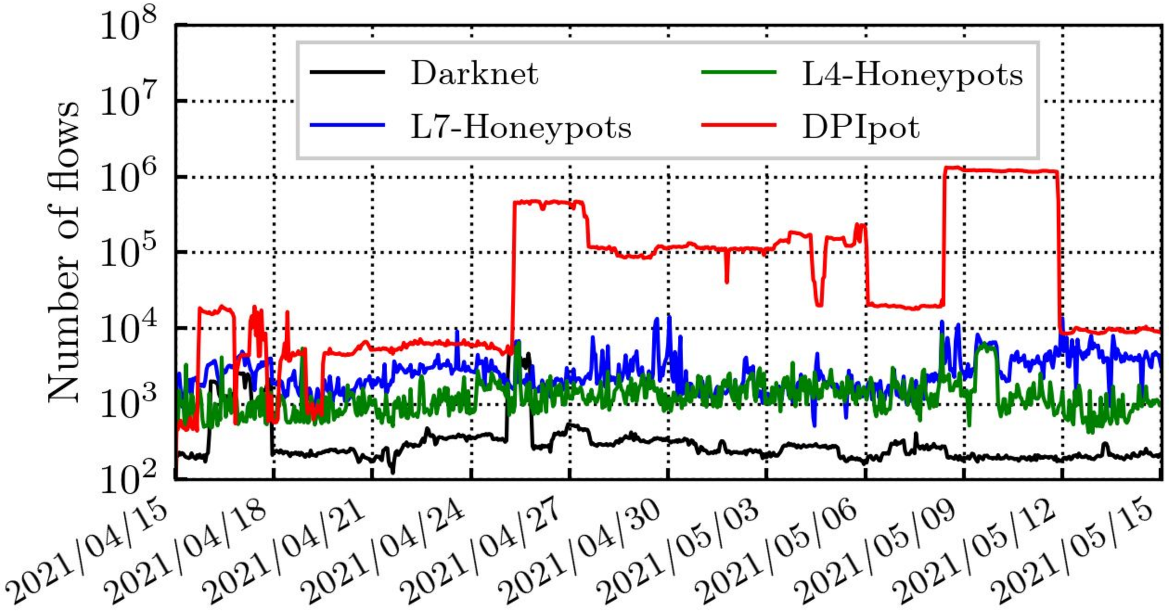
DPIpot: redirecting the attacks to the **most suitable honeypot**



Analysis of the incoming traffic

Q: What is the share of the traffic that arrives to different attack phases?



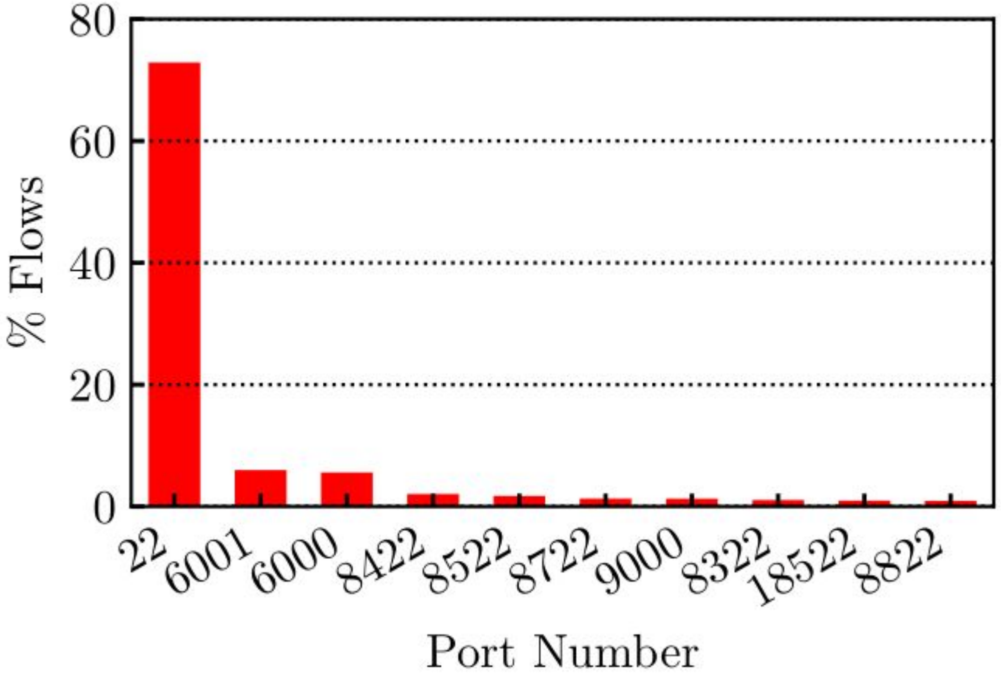


Increment in traffic when we start replying

Analysis of the incoming traffic

Q: Does identifying protocols on-the-fly influence the attack patterns?

SSH



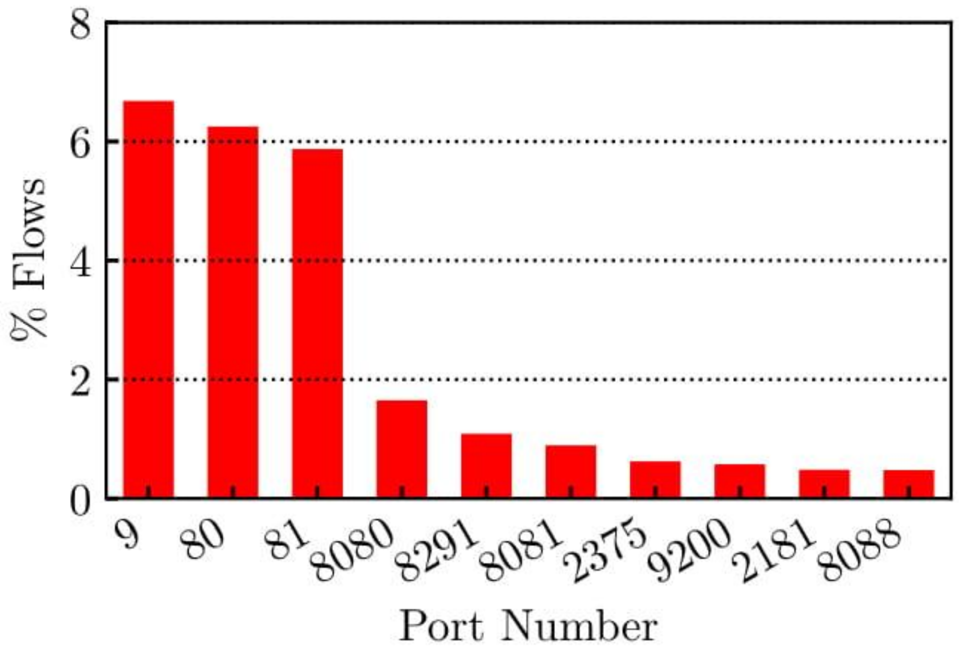
- 119 k flows
- 1097 source IPs
- 187 destination ports

We observe that most of the traffic reaches the standard port

Analysis of the incoming traffic

Q: Does identifying protocols on-the-fly influence the attack patterns?

HTTP

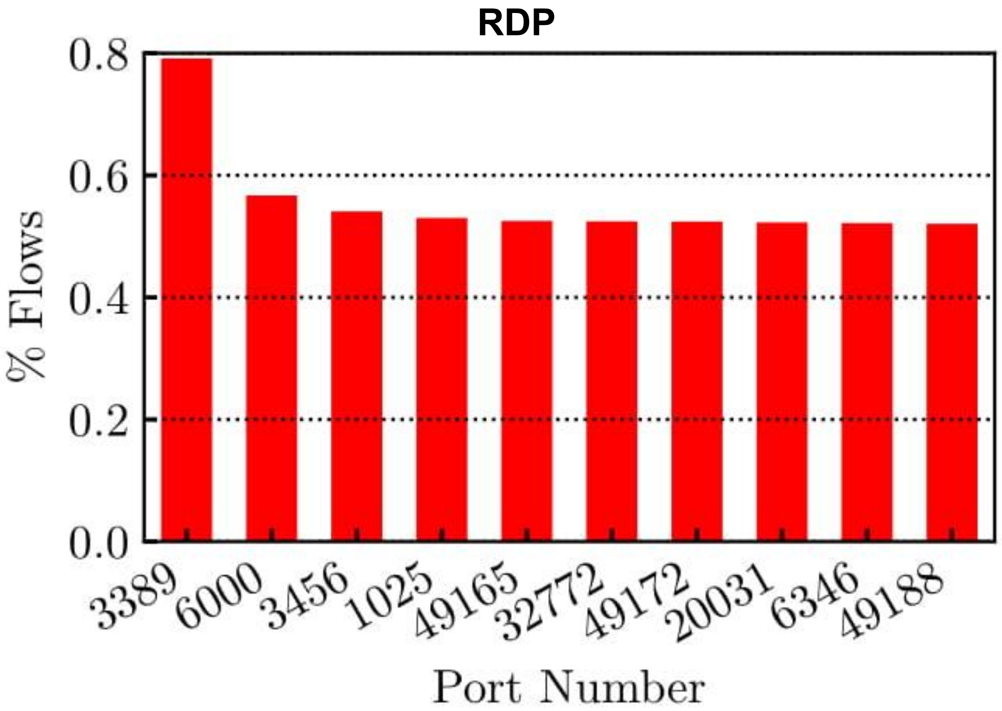


- 444 k flows
- 13 k source IPs
- 9 k destination ports

We observe that attacks on non-standard ports are common for HTTP

Analysis of the incoming traffic

Q: Does identifying protocols on-the-fly influence the attack patterns?



- 329 M flows
- 1415 source IPs
- 28 k destination ports

We observe that attacks on non-standard ports are very common for RDP

Conclusions

- Expected **increase in traffic** when active services are deployed on the darknet
- **Scanning attempts** attracted by opening different services both on standards and nonstandard ports
- Combining the several interaction levels **augments visibility**
- The large amount of collected information calls for **automatic methods** for analyzing the data

Thank you!

Questions?