ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

XXXV Cycle

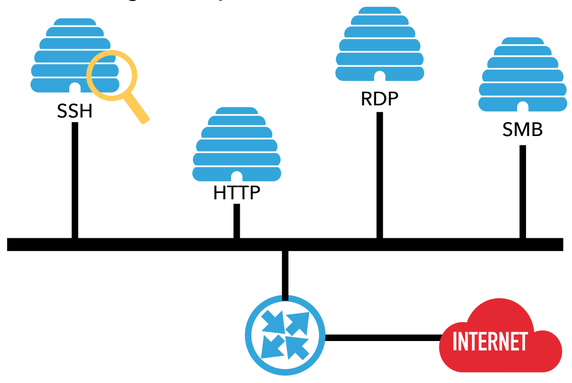
What scanners do at L7? Exploring Horizontal Honeypots

Thomas Favale

Supervisor: Prof. Marco Mellia & Prof. Danilo Giordano

Research context and motivation

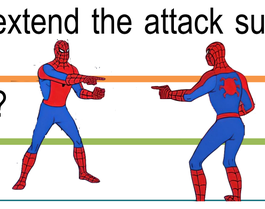
- **Honeypots** are a common means to collect data useful for threat intelligence.
  - The goal is to **engage with the attackers** with either emulators:
    - Replicate basic functions of real systems (low-interaction honeypots)
    - Fully-working live systems deployed in controlled environments (high-interaction honeypots)
- Most efforts in this area rely on **vertical systems** and target a specific scenario or service to analyse data collected in such deployment.



- Well established projects already available
  - TPot, "The all in one honeypot platform": https://github.com/telekom-security/tpotce

Addressed research questions/problems

- I define **attackers** all IP sources that generates **application level traffic** to an Honeypot
- I revisit the visibility from an horizontal perspective:
  - Do attackers typically attack a **single system** or do they extend the attack surface on **multiple systems**?
    - Do they use the same **strategies** for multiple honeypots?
  - How **traffic changes** from a temporal point of view?

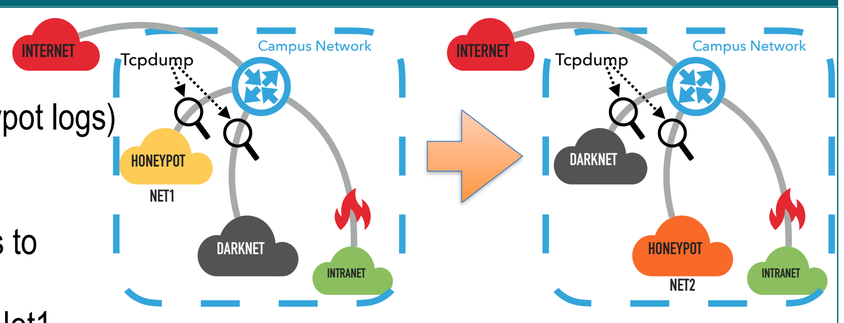


Novel contributions

- I show how attackers are **fast in discovering** and trying to abuse the infrastructure.
- I identify different groups of attackers:
  - Those who perform **large-scale attacks against single services**
  - Others who focus on **horizontal attempts against all services**.
- I evaluate the passwords used in **brute-force** login attempts and identified:
  1. Attackers relying on well-known password lists
  2. Attackers with completely different sets of passwords.
- The latter ones usually come from different geographic places and focus on particular services.

Adopted methodologies

- I monitor incoming traffic
  - **Packet-level** (Tcpdump)
  - **Application-level** (honeypot logs)



- I perform the following steps to gain discovery patterns:
  - 27/10/2021 activation of Net1
  - 25/01/2022 shut down of Net1
  - 09/02/2022 activation of Net2

Submitted and published works

✦ Favale, T. , Soro, F. , Trevisan, M. , Drago, I. , Mellia, M., "*Campus traffic and e-Learning during COVID-19 pandemic*", Computer networks, vol. 176, 2020

✦ Favale, T. , Trevisan, M. , Drago, I. , Mellia, M., "*α-MON: Traffic Anonymizer for Passive Monitoring*", IEEE Transactions on Network and Service Management, vol. 18, no. 2, 2021, pp. 1233-1245

✦ Soro, F. , Favale, T. , Giordano, D. , Drago, I. , Mellia, M. , Rescio, T. , Ben Houidi, Z. , Rossi, D., "*Enlightening the Darknets: Augmenting Darknet Visibility with Active Probes*", under review at IEEE Transactions on Network and Service Management

✤ Favale, T. , Trevisan, M. , Drago, I. , Mellia, M., "*α-MON: Anonymized Passive Traffic Monitoring*", 32nd International Teletraffic Congress (ITC 32), Osaka, Japan, 2020, pp. 10-18

✤ Jha, N. , Favale, T. , Vassio, L. , Trevisan, M. , Mellia, M., "*Z-anonymity: Zero-delay anonymization for data streams*", IEEE International Conference on Big Data, Atlanta, GA, USA, 2020, pp. 3996-4005

✤ Rescio, T. , Favale, T. , Soro, F. , Mellia, M. , Drago, I., "*DPI Solutions in Practice: Benchmark and Comparison*", IEEE Security and Privacy Workshops, San Francisco, CA, USA, 2021, pp. 37-42

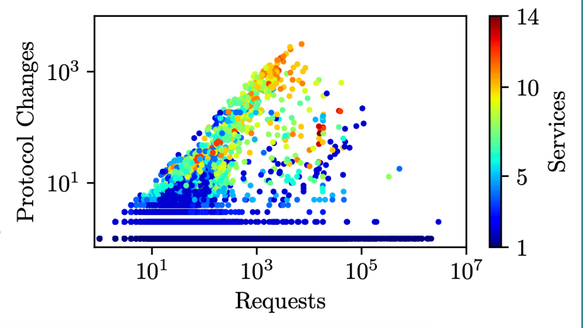
✤ Favale, T. , Giordano, D. , Drago, I. , Mellia, M., "*What Scanners do at L7? Exploring Horizontal Honeypots for Security Monitoring*", IEEE European Symposium on Security and Privacy Workshops, Genoa, Italy, 2022, pp. 307-313

✤ Geissler, S. , Lutu, A. , Wamser, F. , Favale T. , Vomhoff, V. , Krolikowski, M. , Perino, D. , Mellia, M. , Hossfeld, T., "Untangling IoT Global Connectivity: The Importance of Mobile Signaling Traffic", under review at ACM MobiCom (Annual International Conference On Mobile Computing And Networking).

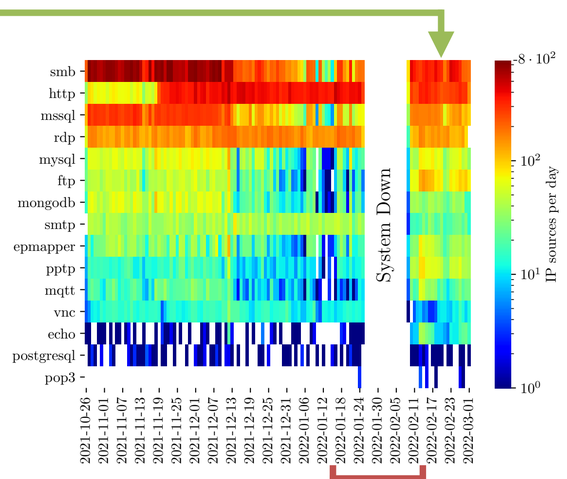
✶ Soro, F. , Favale T. , Giordano, D. , Vassio, L. , Ben Houidi, Z. , Drago, I., "*The New Abnormal: Network Anomalies in the AI Era*", Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning, 2021, pp. 261-288

Results

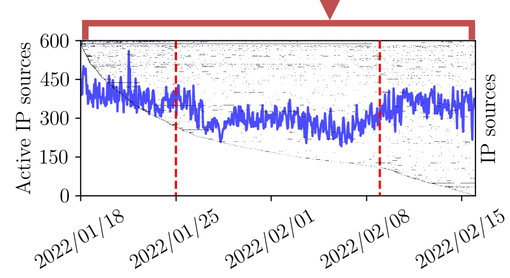
- Vertical vs Horizontal activity
  - Multiple sources keeps **rotating regularly** over multiple services: Horizontal Scanners
  - Some particularly active sources are associated to security crawlers



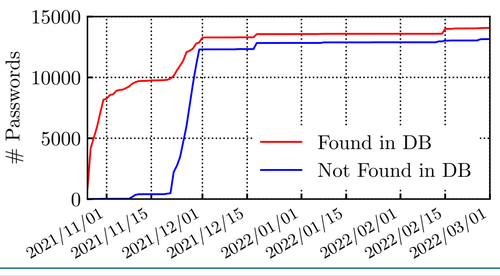
- Evolution over time
  - Traffic pattern is highly **irregular**
  - After shutdown traffic pattern is similar to before



- **Attackers return** over time
  - Old and new attackers continue to search for honeypots when offline
  - As soon as the systems is active, attackers discover them



- Passwords Brute Force Attacks
  - Use of **well-known** passwords is extensive
  - **New datasets** can emerge and may have short life



Future work

- **Extension** of the infrastructure to other honeypots and locations
- Creation of **open honeypot datasets**
- Build updated **profiles of active attackers**, using automated methodologies

PhD Career

- Focus on **Network Traffic Anonymization** and **Data Analysis** for **Cybersecurity** purposes
- Collaboration with *Huawei Technologies*, *Telefonica*, *GARR* and *Intesa Sanpaolo*

List of attended classes

- 01UJBRV - Adversarial training of neural networks (1/7/2020, 15 Hard)
- 01TRARV - Big data processing and programming (1/3/2022, 20 Hard)
- 02LWHRV - Communication (16/11/2019, 5 Soft)
- 01QTEIU - Data mining concepts and algorithms (20/1/2020, 20 Hard)
- 01UJARV - Data science for networks (23/7/2020, 20 Hard)
- 01PJMRV - Etica informatica (4/5/2020, 20 Soft)
- 01UKDRO - Introduction to history of science (11/6/2020, 20 Hard)
- 01UJVRS - IoT platforms for spatial analytics in smart energy systems (19/5/2020, 25 Hard)
- 01UNTRV - Managing conflict: negotiation and communication (2/7/2020, 5 Soft)
- 01UNVRV - Navigating the hiring process: CV, tests, interview (9/2/2021, 2 Soft)
- 01UNYRV - Personal branding (16/12/2020, 1 Soft)
- 01ULSRS - Psycology of urban life (13/2/2020, 10 Hard)
- 01RISRV - Public speaking (4/1/2020, 5 Soft)
- 01QRPRV - Satellite Navigation signal exploitation for atmospheric and environmental monitoring (9/11/2020, 15 Hard)
- 01UKBRV - Space Networking (didattica di eccellenza vp) (1/4/2020, 20, Hard)
- 01UNXRV - Thinking out of the box (20/11/2020, 1 Soft)
- 01SWPRV - Time management (7/12/2019, 2 Soft)

POLITECNICO DI TORINO

PhD program in
Electrical, Electronics and Communications Engineering