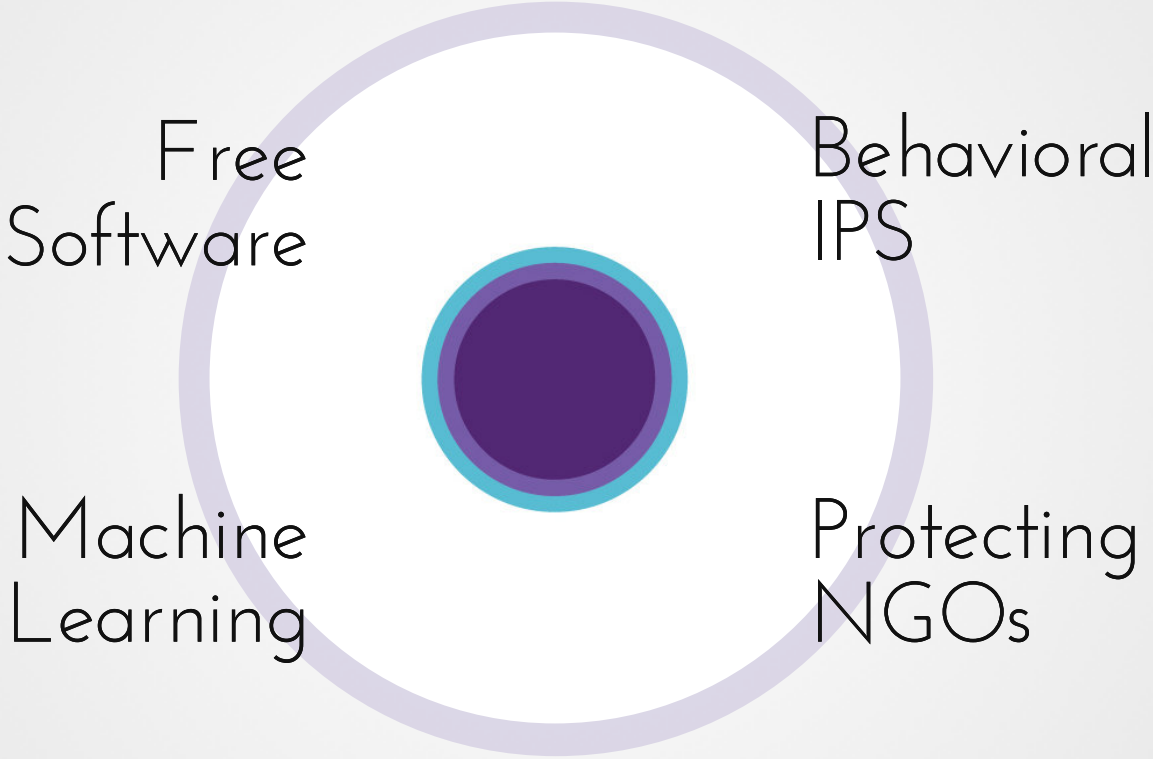
Malware behavior in the Network. A deep analysis with Machine Learning

KONFERENCE
INTERNET
A TECHNOLOGIE
16

Sebastian Garcia
@eldracote
sebastian.garcia@agents.fel.cvut.cz
https://stratosphereips.org

bit.ly/mbitn

Stratosphere IPS (CVUT)



https://stratosphereips.org/

A Cornucopia of Malware

- ~500,000 new malware per day [1][2].
- IP address? domains?

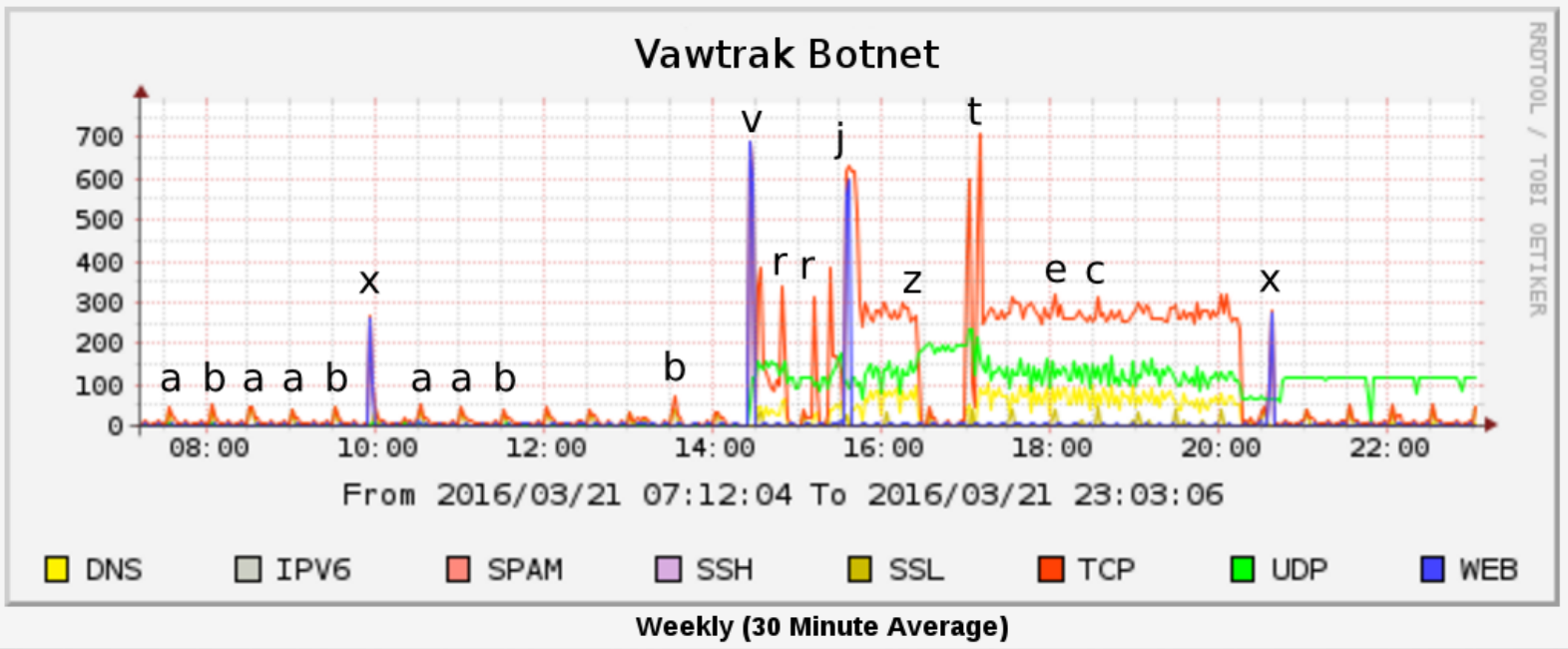
- The protocols used to communicate are considerable less.
- The **behaviors** in the networks, the *how*, are even less.

[1] https://www.av-test.org/en/statistics/malware/

[2] http://blog.trendmicro.com/malware-1-million-new-threats-emerging-daily/

Stratosphere IPS

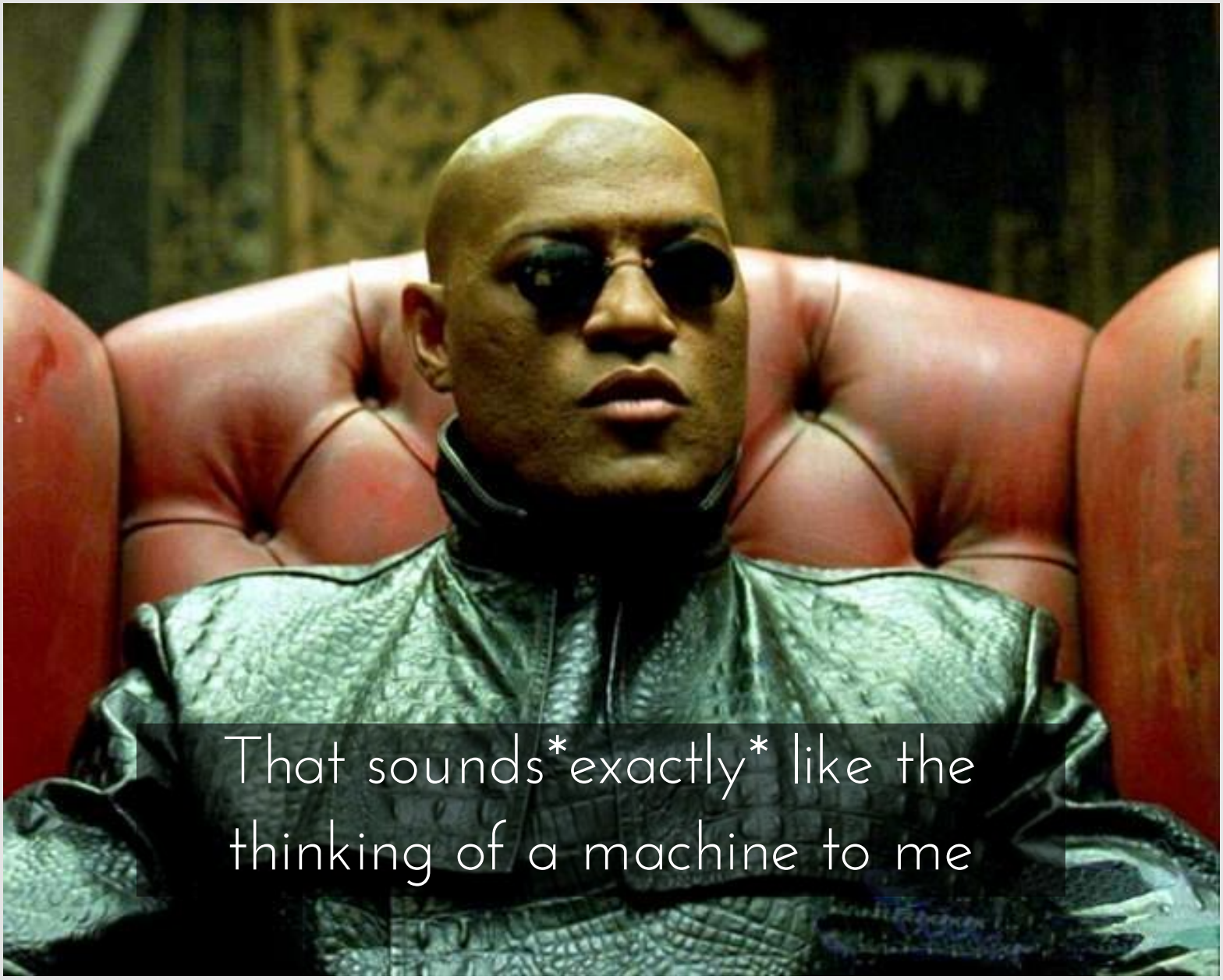
- Work with **flows**, not data.
- Model network behaviors as a string of **letters**.
- **1** flow → **3** features → **1** letter



Behavior of some Usual Suspects. Demo

- Geodo (https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-122-1/)
  - 14 C&C IPs
  - Freq: 3:20mins and 17:20mins

- Upatre (https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-162-1/)
  - 50 C&C IPs
  - 1 minute between one IP and the next.
  - Freq: 34mins _exactly_ again to the same IP.


That sounds*exactly* like the
thinking of a machine to me

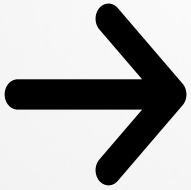
What to do with these behaviors?

Markov Chains Models

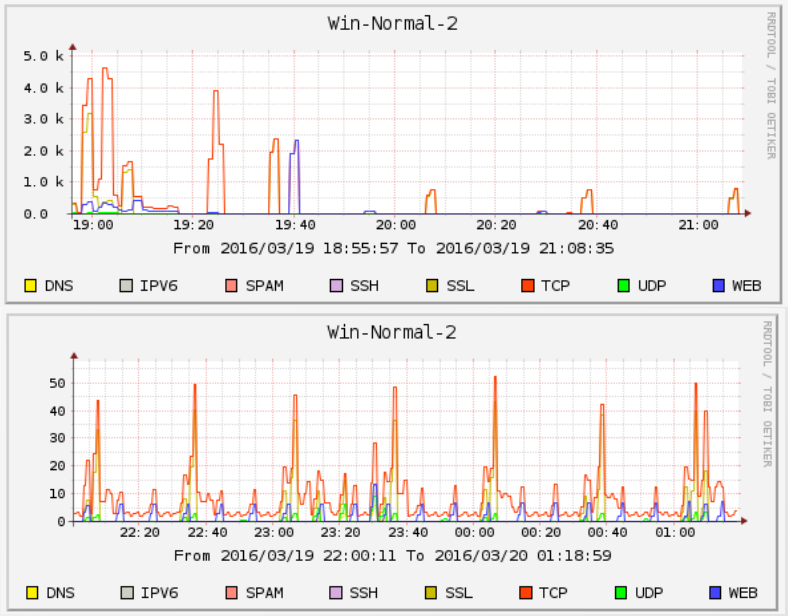
- Create, train and store a Markov Chain models

Behavioral Detection

Trained
Markov Models



Similarity to
Unknown Traffic



Conclusion

- Malware can have very identifiable **behaviors**.
- The behaviors are useful for **analysis and verification**.
- The behaviors are useful for **detection**.
- Behavioral **Machine Learning** is improving.
- Stratosphere is offered as a free cloud-based service for NGOs.

Questions? And Thanks!

Interested in collaborating?

Sebastian Garcia

sebastian.garcia@agents.fel.cvut.cz

@eldracote

https://stratosphereips.org