Hack The Hacker

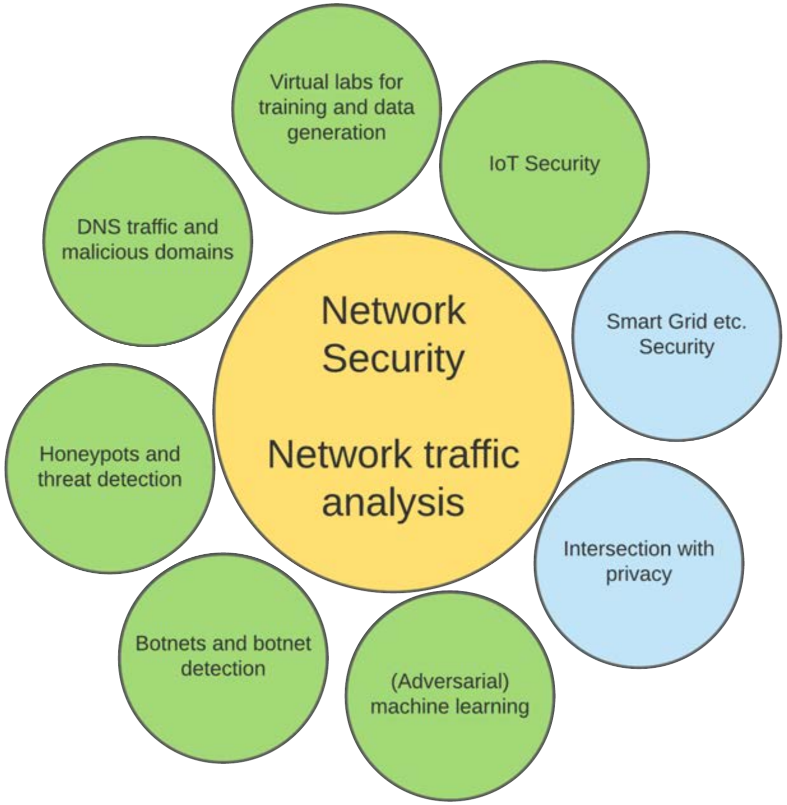
Prof. Jens Myrup Pedersen

Aalborg University (Copenhagen)

AALBORG UNIVERSITY
DENMARK

The next 25 minutes

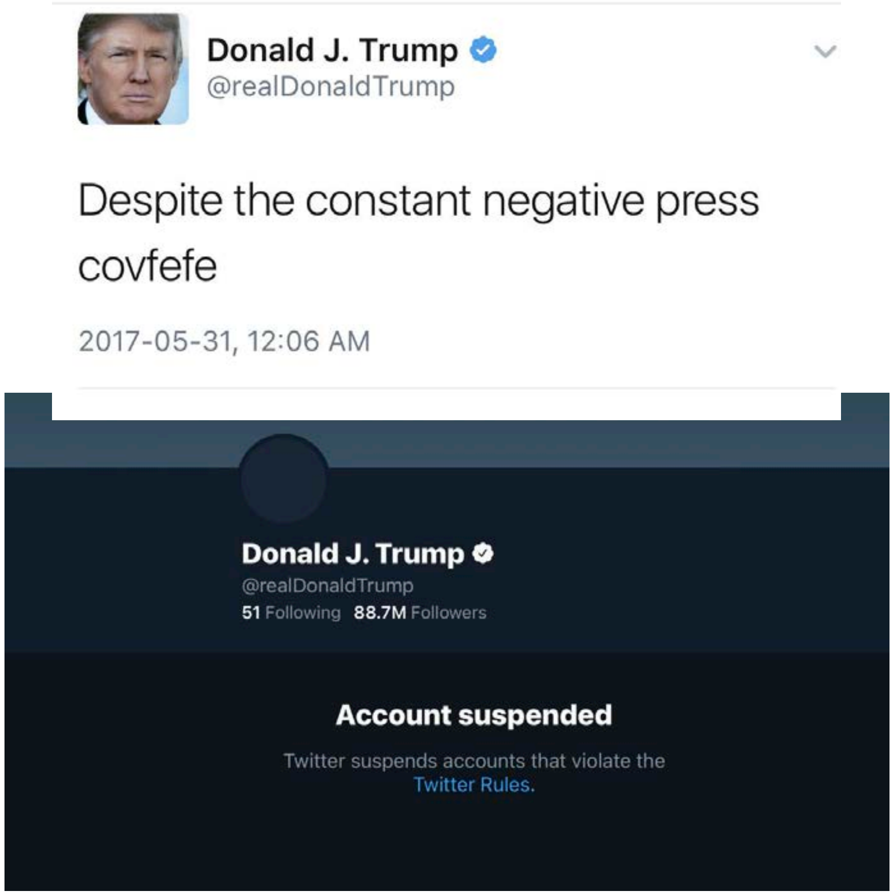
- What are the problems we are up against?
- Cyber attacks and the attackers
- Our research!
- Looking into the future


Network Security
Network traffic analysis
Virtual labs for training and data generation
IoT Security
DNS traffic and malicious domains
Smart Grid etc. Security
Honeypots and threat detection
Intersection with privacy
Botnets and botnet detection
(Adversarial) machine learning

AALBORG UNIVERSITY
DENMARK

The problems!

- We are increasingly dependent on digital infrastructure and services.
- We know too little about the attacks going on (even though it is improving).
- We are up against malicious actors, whom are adopting their strategies according to the countermeasures taken.
- It's an asymmetric battle.
- Attacks such as SolarWinds, Maersk and Demant are scary and fascinating, but the smaller attacks are just as important!
- We need to make realistic assumptions ☺



Donald J. Trump
@realDonaldTrump

Despite the constant negative press covfefe

2017-05-31, 12:06 AM

Donald J. Trump
@realDonaldTrump
51 Following 88.7M Followers

Account suspended

Twitter suspends accounts that violate the Twitter Rules.

AALBORG UNIVERSITET

Knowing the attackers

- We need to understand their:
  - Motivations
  - Resources
  - Capabilities

- Differentiate between:
  - Cyber criminals (for profit)
  - Nation states (strategic)
  - Insiders
  - Greyhats, hacktivists, script kiddies...

Cyber criminals

University of Utah Pays $457K After Ransomware Attack

KRIMI

Tidligere terrordømte hackede sig til millioner på biblioteker

1. feb. 2019, 11:50
Opd. 1. feb. 2019, 13:05

Herlev Bibliotek, Skanderborg Bibliotek og Middelfart Bibliotek var blandt de biblioteker, hvis computere blev hacket af brødrene. Foto: Morten Germund / Scanpix Denmark

MEST SETE PÅ TV2.DK

UDLAND
Kinesisk virus har bredt sig til Europa

EM HÅNDBOLD
Dybt skuffet Sagosen: - Vi havde en drøm og et mål

DAGENS OVERBLIK
Dagens overblik: De største stjerner hylder Wozniacki

EM HÅNDBOLD
Nu starter udskudt semifinale i kølvandet på

Cybersecurity

Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

By William Turton, Michael Riley, and Jennifer Jacobs
13 May 2021, 16:15 CEST
Updated on 14 May 2021, 01:01 CEST

- ▶ Payment came shortly after attack got underway last week
- ▶ FBI discourages organizations from paying ransom to hackers

Damn fine TV
Twin Peaks returns
Exclusive Kyle MacLachlan interview
+ The original cast: what happened next
guide special →

Delicious spring veg recipes
→ cook and weekend

How to be a dad by Tim Dowling (and sons)
→ weekend

Write that novel! The 13 steps to success
→ review

£2.90
Saturday 13.05.17
Published in London and Manchester
theguardian.com

£1.60 for subscribers page 24 →

theguardian

NHS targeted in global cyber-attack

- ● Hack appears to exploit US spy agency leak
- ● Major incident declared as 16 NHS trusts hit
- ● Similar strikes reported across Europe and Asia

[illegible]

Continued on page 3 →

He's looking for the C-word ... it's on the door

Theresa May is clearly dominating her party's election campaign, with barely any mention of the Conservatives on their battle bus, which rolled into Northumberland yesterday Photograph: Stefan Rousseau/PA

Don't turn May into Thatcher, warns Tom Watson

Anushka Asthana
Political editor

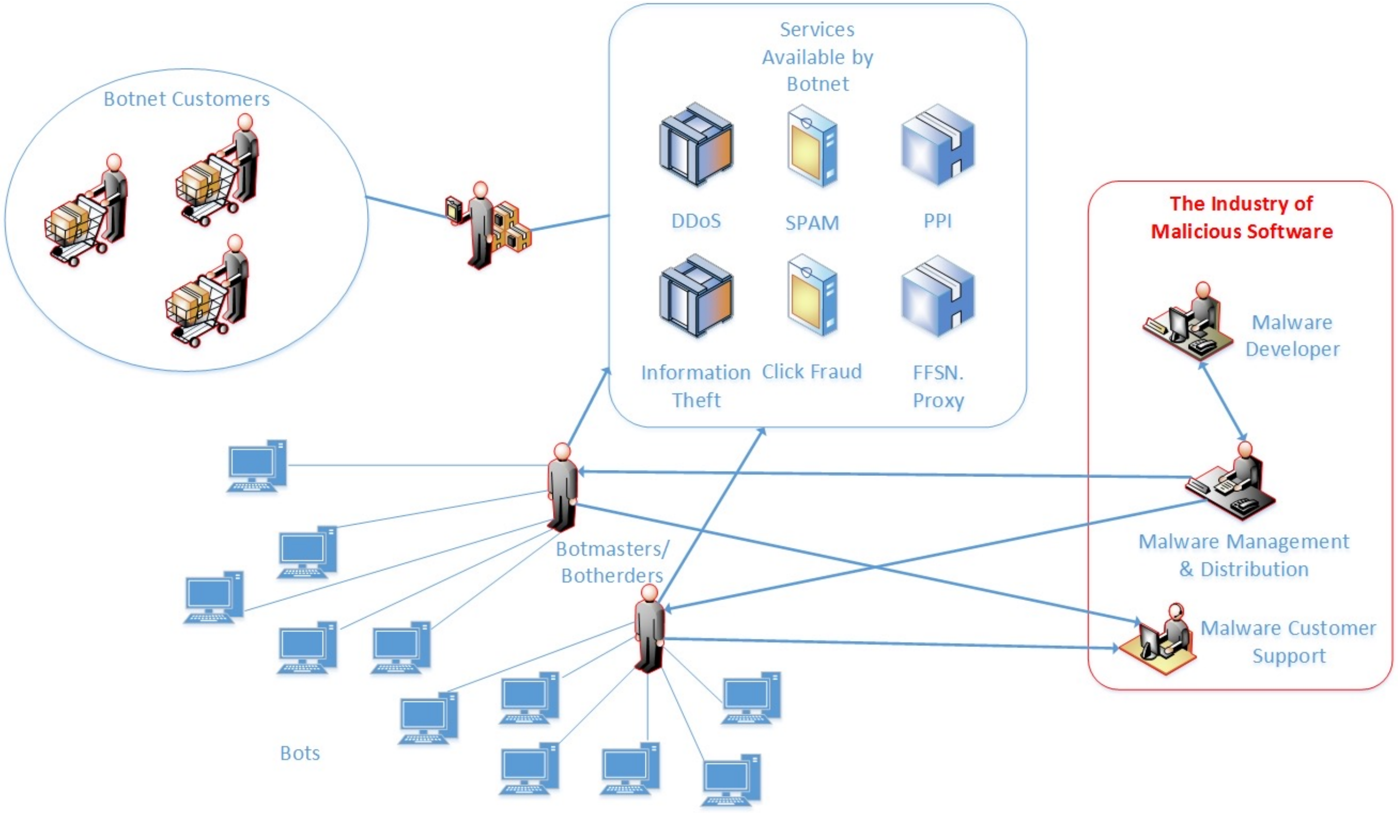
[illegible]

Labour is determined to turn its poor poll numbers around to avoid the Tories winning a sweeping majority of seats, Tom Watson said

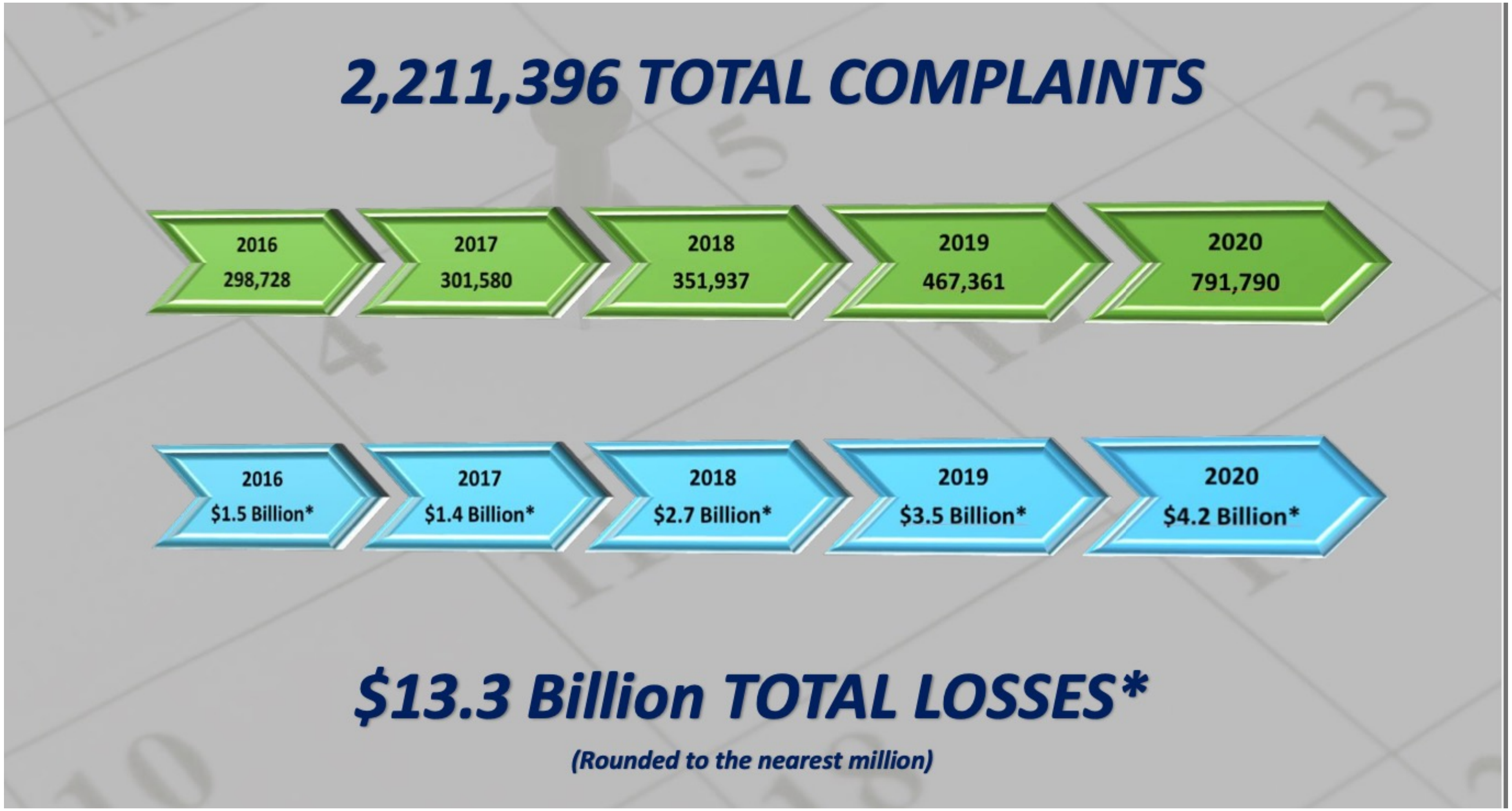
Continued on page 8 →

First it was a lettuce shortage, then a courgette crisis. Now there is trouble looming in the avocado aisle...
Full story, page 5 →

Cyber criminals - markets



Losses according to Internet Crime Complaint Center (FBI)



2,211,396 TOTAL COMPLAINTS

2016
298,728

2017
301,580

2018
351,937

2019
467,361

2020
791,790

2016
$1.5 Billion*

2017
$1.4 Billion*

2018
$2.7 Billion*

2019
$3.5 Billion*

2020
$4.2 Billion*

$13.3 Billion TOTAL LOSSES*

(Rounded to the nearest million)

Nation States

- Ukraine Power Grid (2015 edt)
- Social engineering in the first step.
- Users open a file, click a link, or give away their credentials.
- Stays inside the system for months, to learn and move between networks and systems.
- Investing ressources in carrying out sophisticated attacks (e.g. development of malicious firmware).

http://www. wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

What do do about the attacks?

NIST framework suggests five functions to protect against cyber attacks:

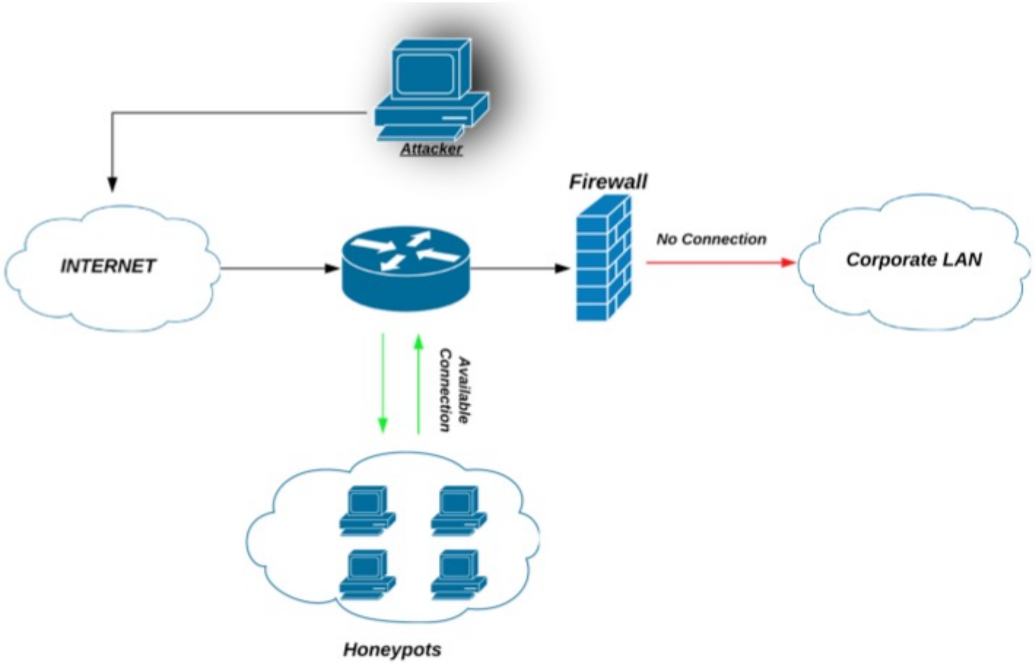
- Identify
- **Protect**
- **Detect**
- Respond
- Recover

Knowing the attacks

- When there is a (big) fire, we learn from it.
- If there is a plane crash, we learn from it.
- If there is a cyber attack, we also need to learn from it.

- Example from our research: Honeypots and deception technologies.

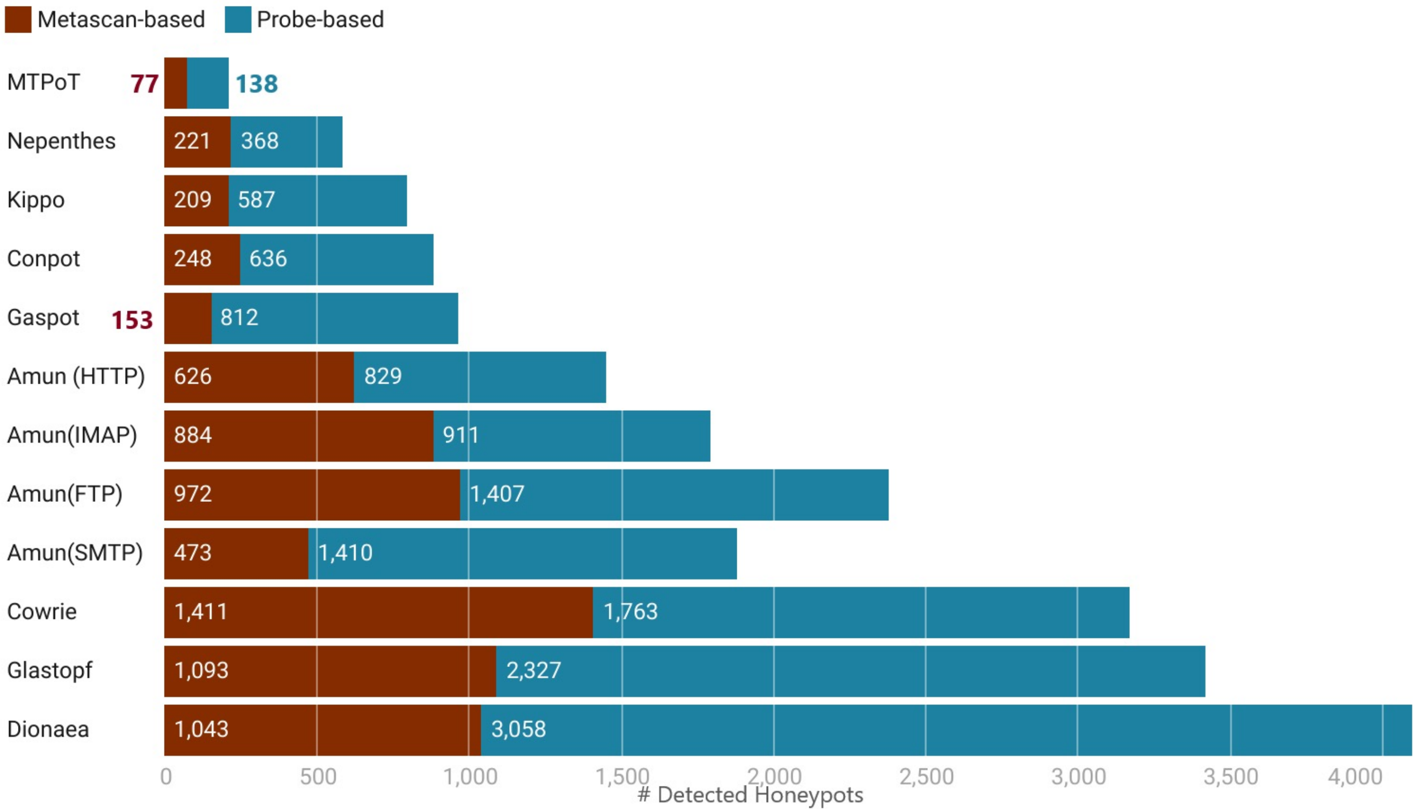
- Creating honeypots and honeytokens that can not be easily detected is a particular challenge.



Mahmoud, R-V., & Pedersen, J. M. (2019). Deploying a University Honeypot: A case study. CEUR Workshop Proceedings, 2443, 27-38. http://ceur-ws.org/Vol-2443/

See also: Srinivasa, S., Pedersen, J. M., & Vasilomanolakis, E. (2021). Towards systematic honeytoken fingerprinting. I International Conference on Security of Information and Networks (ACM SIN) Association for Computing Machinery.

Multistage honeypot fingerprinting

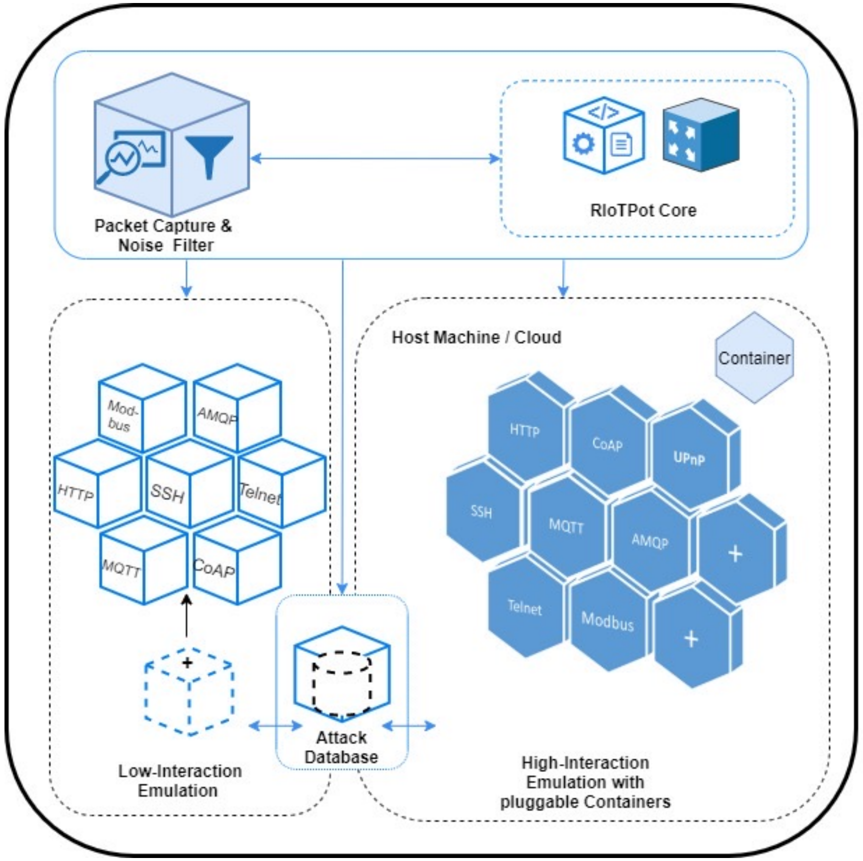


AALBORG UNIVERSITY
DENMARK

Shreyas Srinivasa, Jens Myrup Pedersen and Emmanouil Vasilomanolakis.
Gotta catch' em all: a Multistage Framework for honeypot fingerprinting. (2021).
arXiv.cs.CR/2109.10652

RIoTPot

- Modular design
- Hybrid interaction – low + high interaction
- Focus on IoT and OT environments
- Packet capture
- Noise filter – labelling of traffic received from known scanning services



Srinivasa, Shreyas, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis. **"RIoTPot: a modular hybrid-interaction IoT/OT honeypot."** *26th European Symposium on Research in Computer Security (ESORICS) 2021*. Springer, 2021.

RIoTPot results

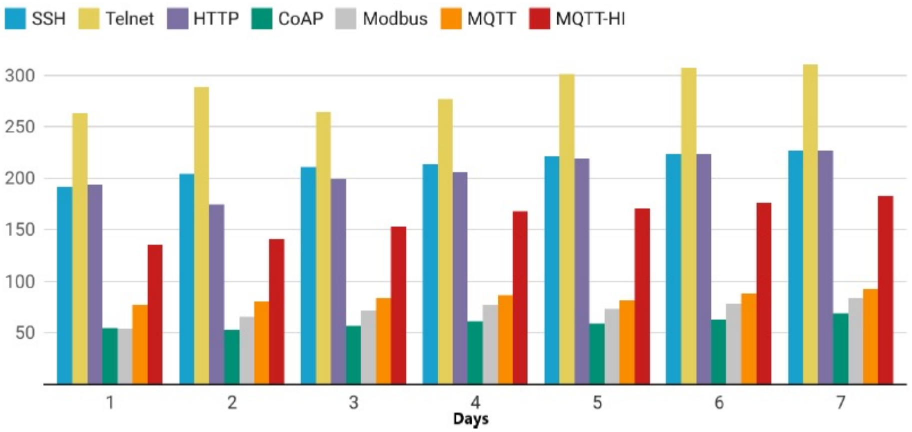


Fig. 2. Number of attacks on protocols per day

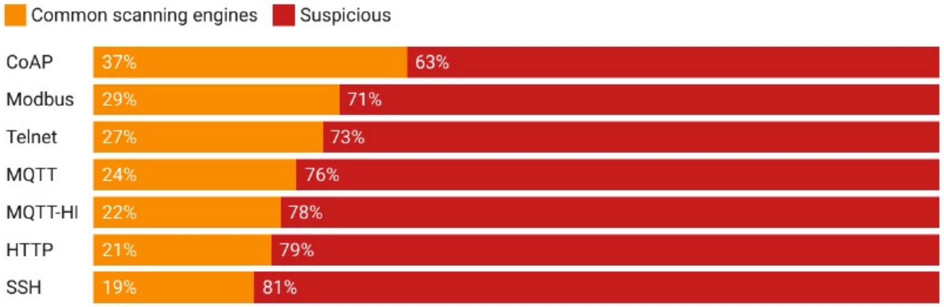


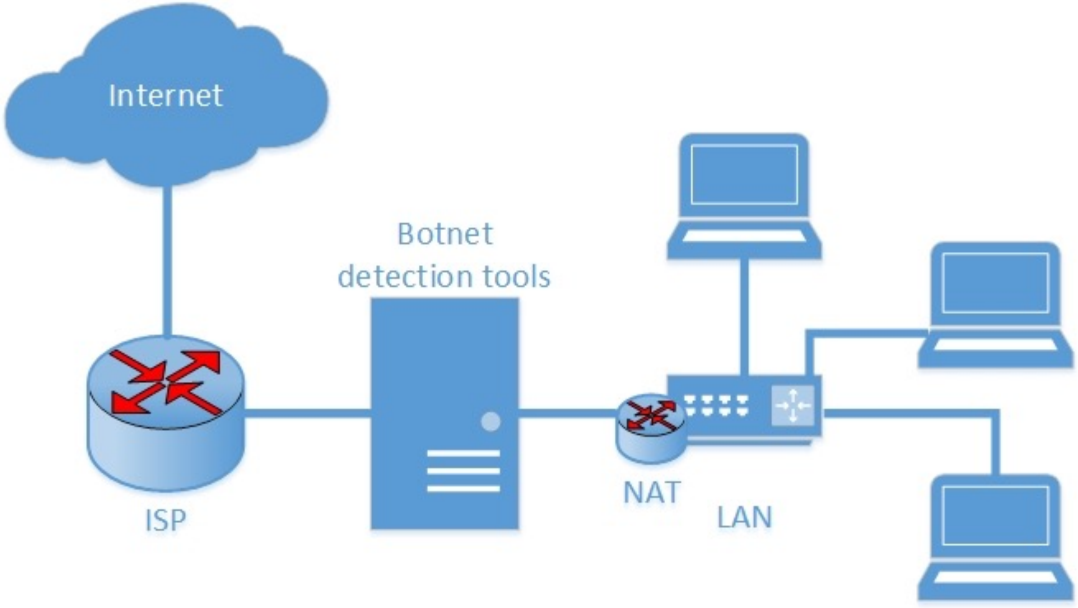
Fig. 3. Attack noise classification in percentage

AALBORG UNIVERSITY
DENMARK

Srinivasa, Shreyas, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis.
"RIoTPot: a modular hybrid-interaction IoT/OT honeypot."
26th European Symposium on Research in Computer Security (ESORICS) 2021.
Springer, 2021.

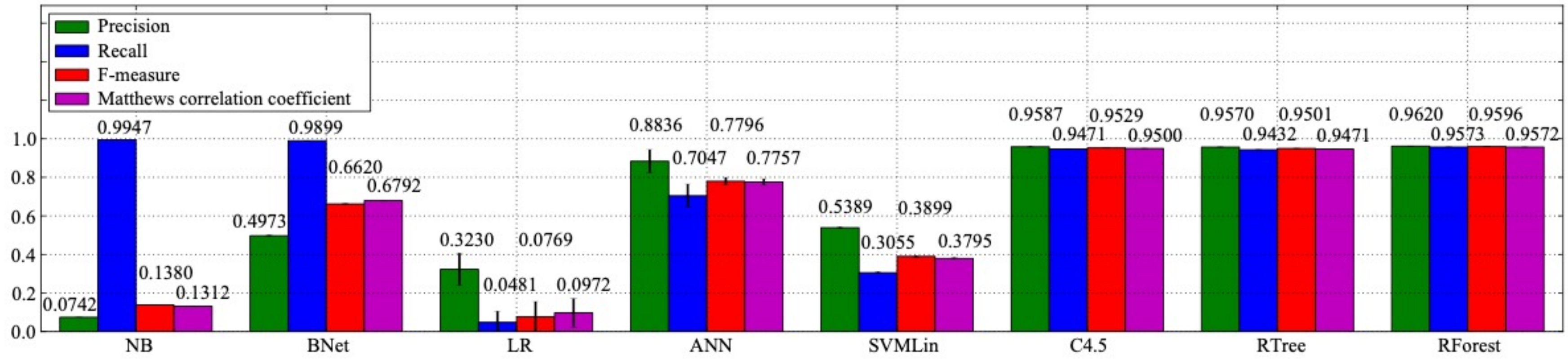
Detection of malicious activities

- There is no silver bullet
- Network-based detection based on machine learning is promising:
  - Not depending on the protection of individual devices.
  - Network traffic can be monitored at different vantage points.
  - Can be based on signatures, rules, or techniques based on Machine Learning.



Machine learning promising, but...

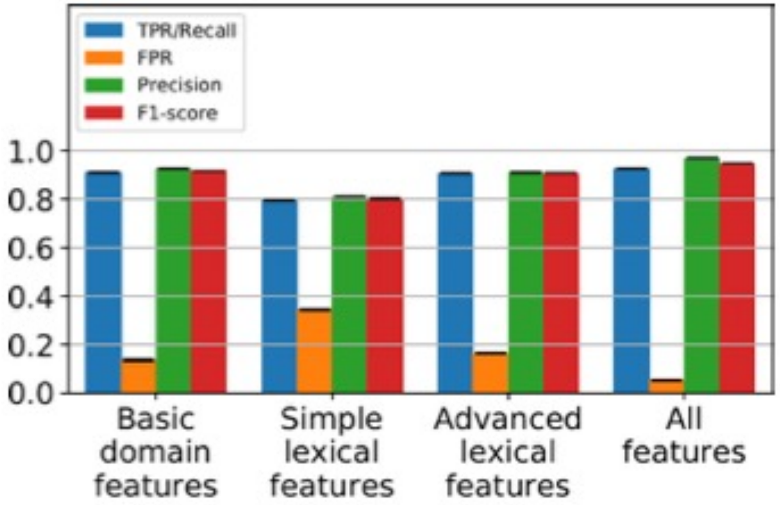
- Getting correctly labelled data sets is challenging
- Are the data representative of the traffic?
- Even a low number of false positives is critical
- How easy is it to cheat our algorithms?



Stevanovic, M., & Pedersen, J. M. (2014). An efficient flow-based botnet detection using supervised machine learning. I Computing, Networking and Communications (ICNC), 2014 International Conference on (s. 797-801). IEEE Press. International Conference on Computing, Networking and Communications https://doi.org/10.1109/ICCNC.2014.6785439

DNS Traffic – lexical analysis

- Basic features, e.g. length of the domain and, Top Level Domain (for example .com, .dk), number of domain levels.
- Simle lexical features, e.g. ratio of consonants in the 2-LD, ratio of special characters in 2-LD, ratio of special characters in 2-LD.
- Advanced lexical features, e.g. Entropy of 2-LD, N-gram analysis of 2-LD, number of English words in 2-LD.
- (but how easy to circumvent for attackers?)
- Currently looking into (1) adding a large number of additional features, and (2) what can be done from different vantage points, e.g. from an ISP point of view.

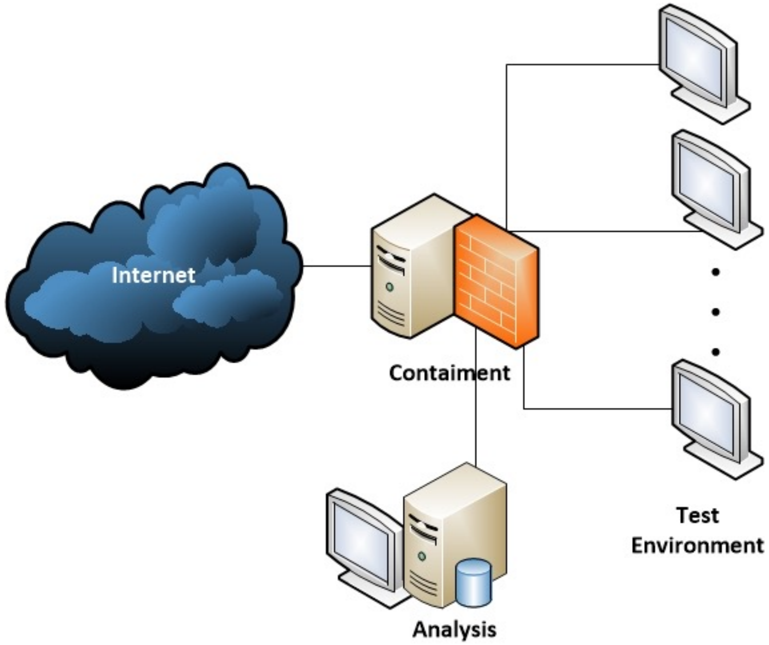


Kidmose, E., Stevanovic, M., & Pedersen, J. M. (2018). Detection of malicious domains through lexical analysis. I 2018 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security) IEEE. https://doi.org/10.1109/CyberSecPODS.2018.8560665

See also ISP point of view: Andersen, M. F., Pedersen, J. M., & Vasilomanolakis, E. (2020). Cyber-security research by ISPs: A NetFlow and DNS Anonymization Policy. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) [9138869] IEEE. https://doi.org/10.1109/CyberSecurity49315.2020.9138869

AAU Star for traffic generation

- Around 300.000 different pieces of malware
- Observing API calls (and in another study domain names)
- We are now ”stepping up” on the sandboxing again, and currently building a new Network Analysis Platform in a PhD project.



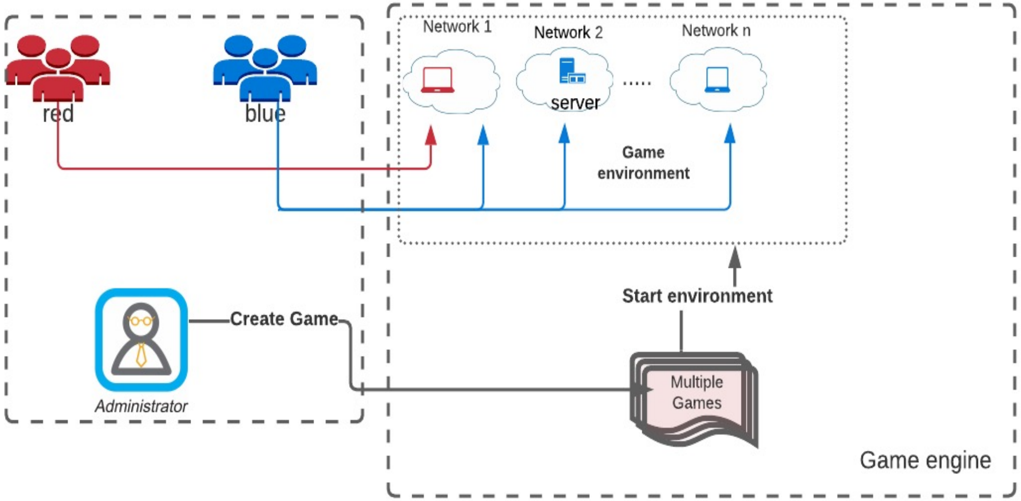
TEKNOLOGIPRISER TIL TELEMEDICIN OG KAMP MOD SKADELIG SOFTWARE

AALBORG UNIVERSITY
DENMARK

Hansen, S. S., Larsen, T. M. T., Stevanovic, M., & Pedersen, J. M. (2016). An approach for detection and family classification of malware based on behavioral analysis. I 2016 International Conference on Computing, Networking and Communications (ICNC) IEEE. https://doi.org/10.1109/ICCNC.2016.7440587

Virtual labs also for training...

- Haaukins for Training in Virtual Labs
- Network Analysis Platform for Red-Team Blue-Team.

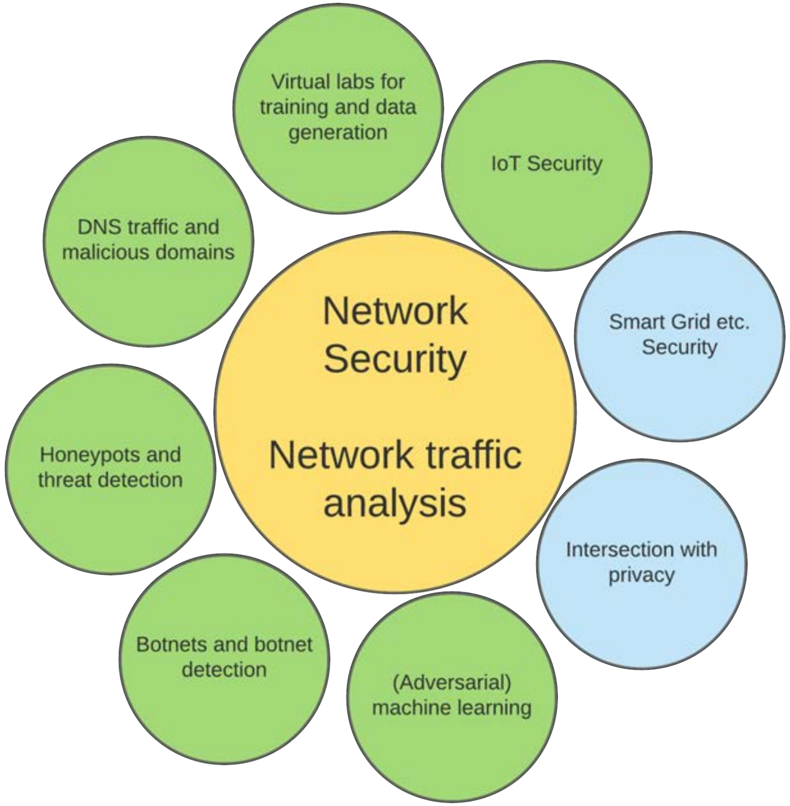


Mahmoud, R-V., Kidmose, E., Broholm, R., Pilawka, O. P., Dominika Illés, D., Magnussen, R., & Pedersen, J. M. (2020). Attack and Defend: Combining Game-Based Learning with Virtual Cyber Labs. I P. Fotaris (red.), Proceedings of the 14th European Conference on Games Based Learning: A virtual Conference hosted by the University of Brighton, UK (s. 364-371). Academic Conferences and Publishing International. https://doi.org/10.34190/GBL.20.150

Panum, T. K., Hageman, K. D., Pedersen, J. M., & Hansen, R. R. (2019). Haaukins: A Highly Accessible and Automated Virtualization Platform for Security Education. I M. Chang, D. G. Sampson, R. Huang, A. S. Gomes, N-S. Chen, I. I. Bittencourt, K. Kinshuk, D. Dermeval, & I. M. Bittencourt (red.), 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT) (s. 236-238). [8820918] IEEE. International Conference on Advanced Learning Technologies (ICALT) https://doi.org/10.1109/ICALT.2019.00073

So this is our path...

- Trends: We need robust methods (due to adversary behavior), increased used of encryption, increased amount of data, increased amont of devices.
- Detection of malicious domains: Extend research with new types of data, improve classification of ifferent kinds of malicious activities.
- Virtual labs – we need data.
- Threats against (and from) IoT devices and OT-systems lead to new threats: Suitable for network based detection of malicious activities. Identity and Access Management.
- Threat detection including Honeypots and IoT honeypots – how can data from honeypots be combined with other sources of data?


Network Security
Network traffic analysis
Virtual labs for training and data generation
IoT Security
Smart Grid etc. Security
Intersection with privacy
(Adversarial) machine learning
Botnets and botnet detection
Honeypots and threat detection
DNS traffic and malicious domains

AALBORG UNIVERSITET

Thank you for your attention

AALBORG UNIVERSITY
DENMARK