DREAMLAB
TECHNOLOGIES

Dreamlab Technologies
SAPPAN

2021 | Bern

> whoami

- Mischa Obrecht, 33
- IT-Security since 9 years, analyst, engineer, project / security manager, tester
- Pentester and project manager for Dreamlab
- Involved in SAPPAN as project coordinator for Dreamlab

To get in touch please use:

- mischa.obrecht@dreamlab.net

Outline

High level overview

Spotlight on two interesting aspects of SAPPAN

- DGA detection using machine learning
- Anonymization and privacy concerns

Pitch for participation in end user commitee

SAPPAN – General Information

Sharing and **A**utomation for **P**rivacy-**P**reserving **A**ttack **N**eutralization

H2020 Call SU-ICT-01-2018 (IA) - Dynamic countering of cyber-attacks:

- **scope:** Cyber-attacks management – advanced response and recovery.
- **timeline**: May 2019 until April 2022.

Abstract:

- Platform for sharing and automation of privacy preserving response and recovery using advanced data analysis and machine learning.
- Decrease the effort required by a security analyst to find optimal responses to and ways to recover from an attack.
- Within a single organization and across organisations through privacy-preserving data processing and sharing.

Coordinator:

Fraunhofer FIT

Industrial Partners:

Hewlett Packard Enterprise

cesnet

Academia:

RWTH AACHEN UNIVERSITY

MUNI


High level overview

General Aims

Motivation: Intrusion Detection Systems

Example scenario:

- Networks are monitored only within individual organizations.
- Suspicious patterns can trigger alerts.
- Alerts can be resolved by response and recovery actions (“playbooks”).
- New threat may cause new patterns.

Common IDS Challenges:

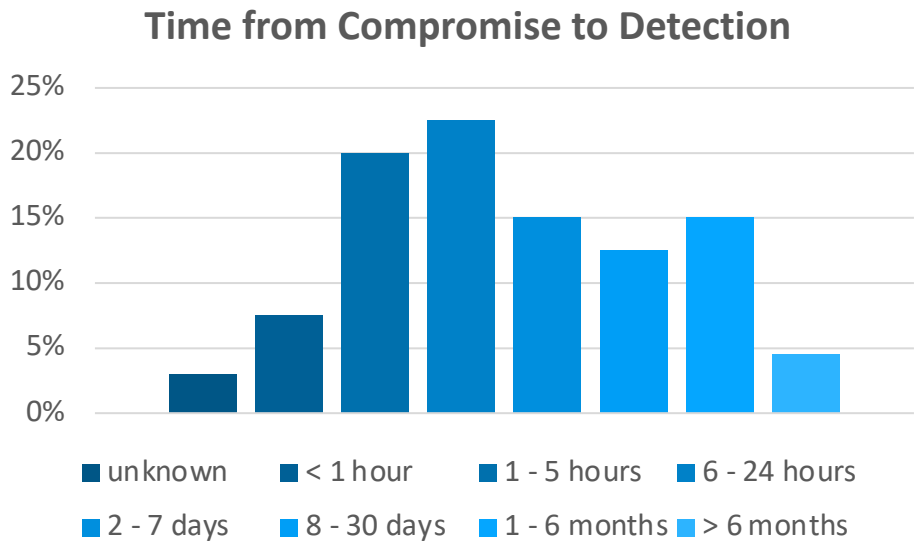
- Limited availability and processed data (e.g., SMEs have less IDS capabilities).
- Difficult to identify attacks with new patterns.
- Too many false positive alerts, security analysts get overwhelmed.
- Data sharing among organizations might lead to privacy/confidentiality leakage.

Motivation:
Long delay in detection of intrusions in the real world

Detection time takes more than 5 hours for two thirds of the cases.

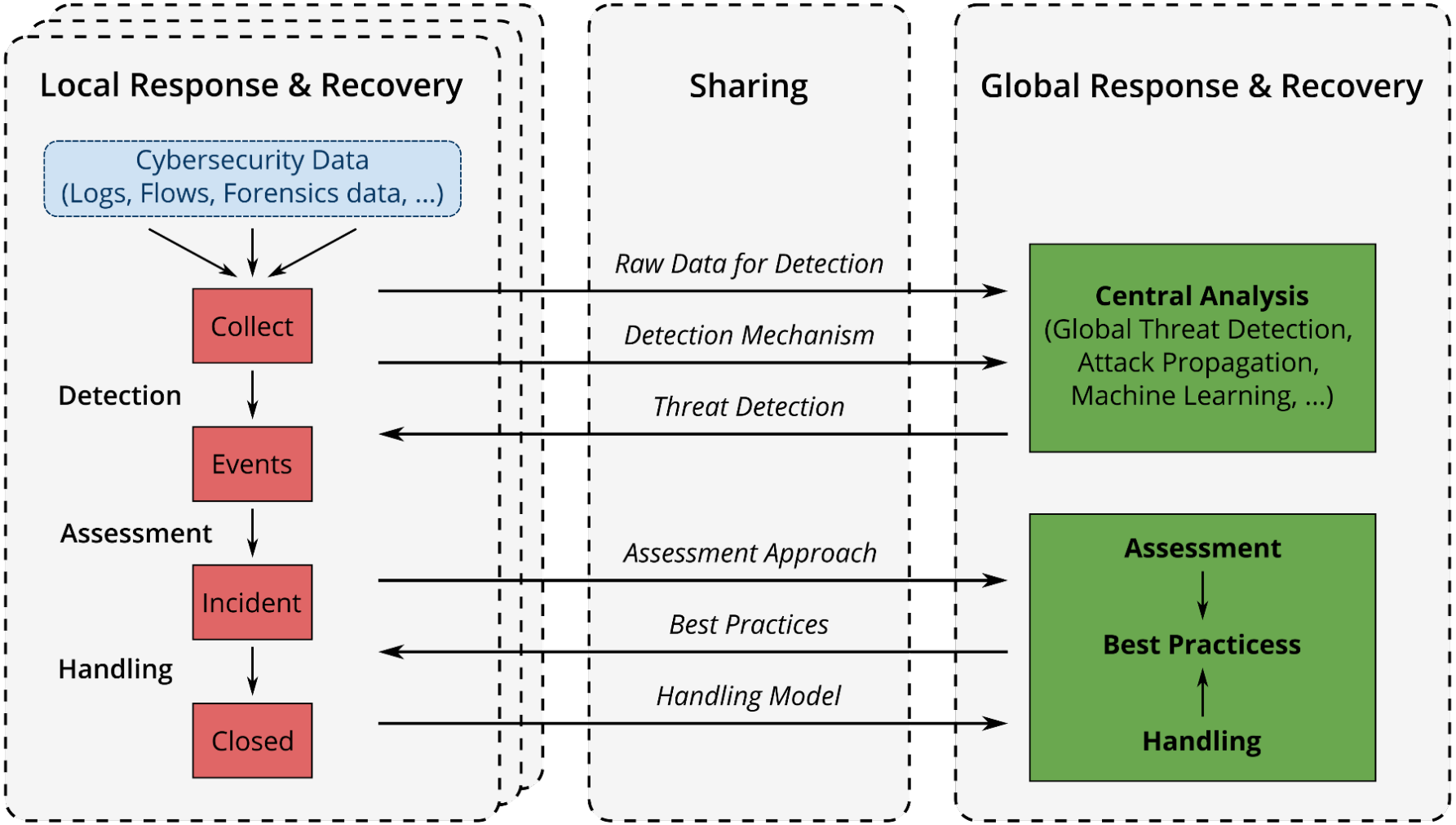
For 20% of cases detection takes more than one month.

Sharing of detection models and actionable response and recovery information between companies could drastically reduce detection and response time.

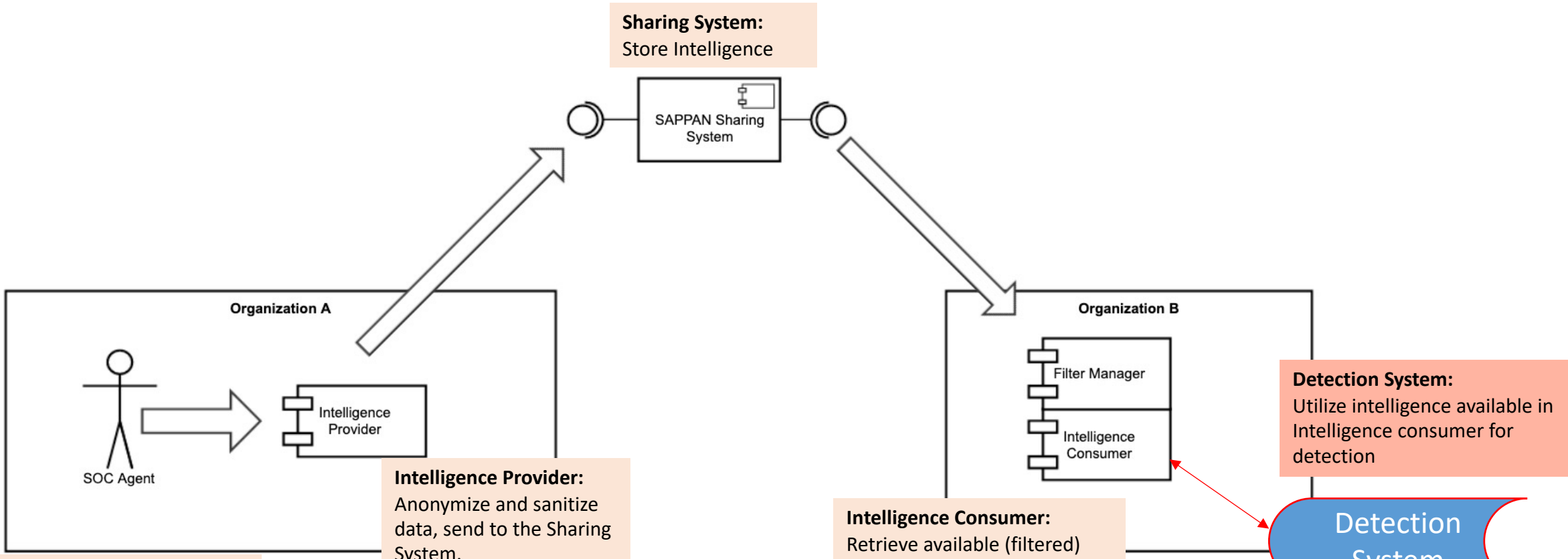


The Show must go on – A SANS Survey by Matt Bromiley – Published 2017 by SANS Institute

SAPPAN Concept



SAPPAN Architecture



Sharing System:
Store Intelligence

Intelligence Provider:
Anonymize and sanitize data, send to the Sharing System.

SOC-Agent: Collect intelligence and publish via Intelligence Provider.

Intelligence Consumer:
Retrieve available (filtered) intelligence from Sharing System

Detection System:
Utilize intelligence available in Intelligence consumer for detection

SAPPAN – Current Progress

- …
- Framework for machine readable playbooks containing response and recovery information
- Research on local detection methods
  - DGA-Detection
  - Classification of phishing URLs
  - Host- and application profiling based on netflow data
- Research on anonymization for sharing of information
- Research on federated machine learning
- …

Spotlight on two interesting aspects of SAPPAN

Local detection methods: DGA detection

Common denominator of many adversaries (especially APTs):

- Initial compromise of victim with malware
- Establishing a “Command and Control”-Channel (C2-Channel)
- Excerting C2 through channel (remote control of malware)

Neuralgic point of attacker:

- Identifying C2 traffic helps to detect malware and block advesarial activities

Local detection methods: DGA detection

IP-adresses or URLs for “calling home” to C2-servers **used** to be hardcoded in malware

➔ Easily detectable! (blacklist)

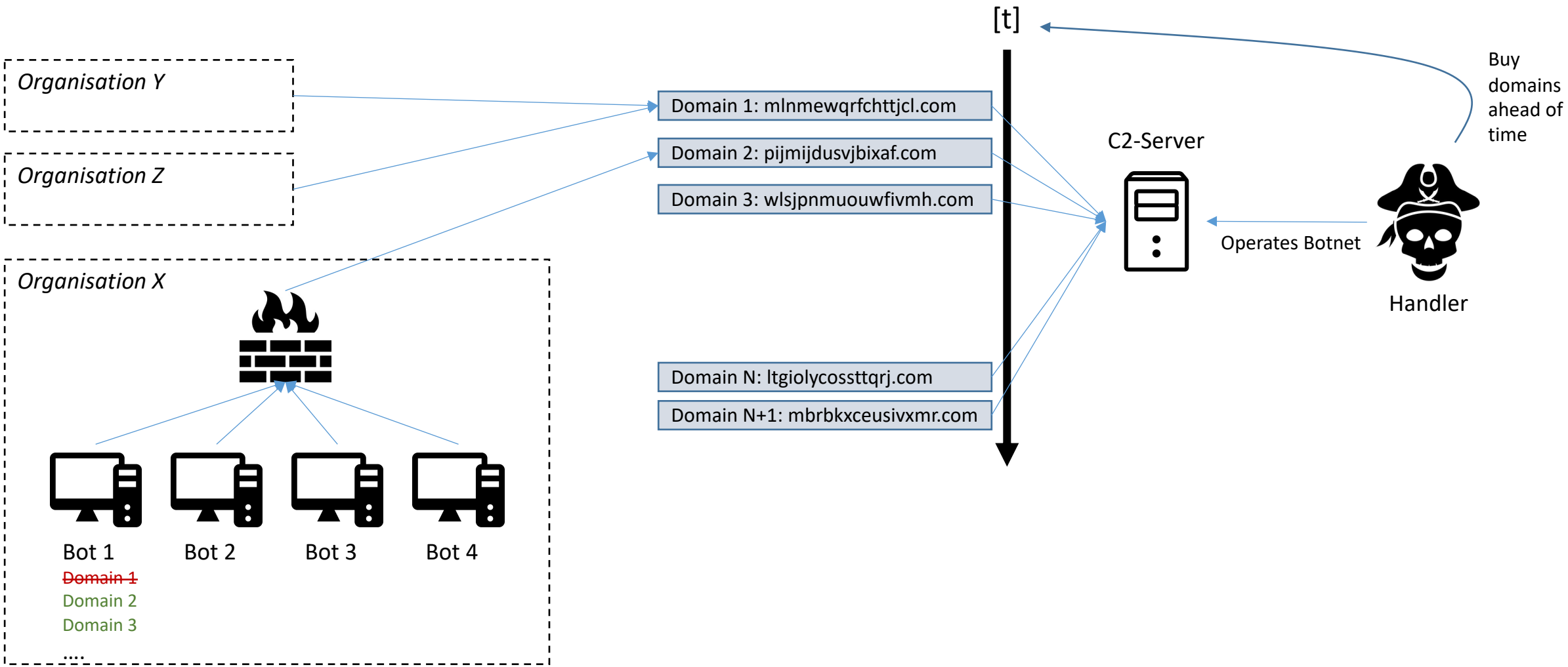
Today:

- Dynamic creation of URLs to phone home to, based on predefined schema / algorithm
- Algorithmically generated domain ➔ Domain generation algorithm (DGA)

Examples:

- *generate_domain(2020,11,12) ➔ ovyvwnkjserklcrj.com*
- *generate_domain(2020,10,1) ➔ mlnmewqrfchttjcl.com*

Local detection methods: DGA detection



Local detection methods: DGA detection

DGAs generate pseudo-random URLs

➔ Try to detect random-”looking” URLs

What does random-”looking” mean?

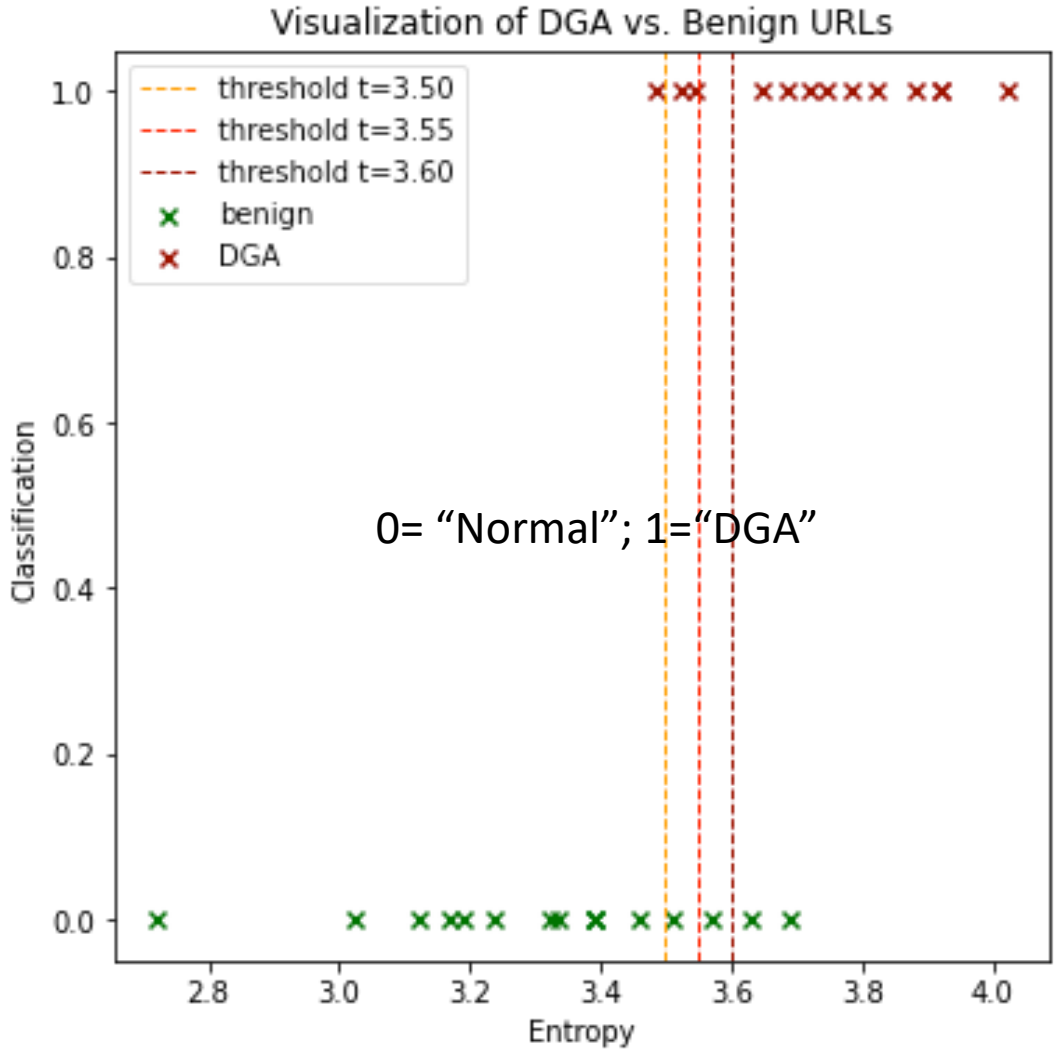
Possible way to make a distinction of generated and “normal” URLs

➔ Entropy! (Shannon, measure of “randomness” of a string)

A classification problem

Local detection methods: DGA detection
Example of DGA classification based on entropy

URL	Type	Entropy
weibu.com	benign	3.1699250014423126
Instagram.com	benign	3.392747410448785
Wikipedia.org	benign	3.3346791410515952
bluewin.ch	benign	3.321928094887362
hao123.com	benign	3.121928094887363
blogspot.com	benign	3.1887218755408675
Microsoftonline.com	benign	3.5110854081804272
wordpress.com	benign	3.238901256602631
cambridge.org	benign	3.392747410448785
facebook.com	benign	3.0220552088742005
netflix.com	benign	3.4594316186372978
amazon.com	benign	2.7219280948873625
stackoverflow.com	benign	3.6901165175936645
Myshopify.com	benign	3.392747410448785
psych-science22.co.uk	benign	3.630412660873997
towardsdatascience.com	benign	3.5726236638951634
ovyvwnkjserklcrj.com	DGA	3.7219280948873616
mlnmewqrfchttjcl.com	DGA	3.646439344671015
pijmijdusvjbixaf.com	DGA	3.746439344671015
wlsjpnmuouwfivmh.com	DGA	3.7841837197791883
ltgiolycossttqrj.com	DGA	3.5464393446710147
jjuyvunkbqidxxcl.com	DGA	3.9219280948873627
tjavhlbnkjxomkmh.com	DGA	3.6841837197791887
mbrbkxceusivxmmr.com	DGA	3.5219280948873615
btbpurnkbqidxxcl.com	DGA	3.8841837197791893
fpptskrsgtknyjmb.com	DGA	3.8219280948873617
ddfjeqpenhvxxusl.com	DGA	4.021928094887363
fheocwdgohfsmlwd.com	DGA	3.484183719779189
ihgjxutqhlgfmwej.com	DGA	3.9219280948873627



Local detection methods: DGA detection

Entropy-based DGA classification:

- Problem 1: What is the right threshold? Does it generalize?
- Problem 2: Chance of wrong classification (false positives)?

Solution/Improvement?

- Usage of machine learning (RESNET, ConvNET) instead of simple thresholding for classification

➔ Big improvement in accuracy:

Method	Accuracy
Entropy based	49% - 71%
ML (SAPPAN)	69% - 99%

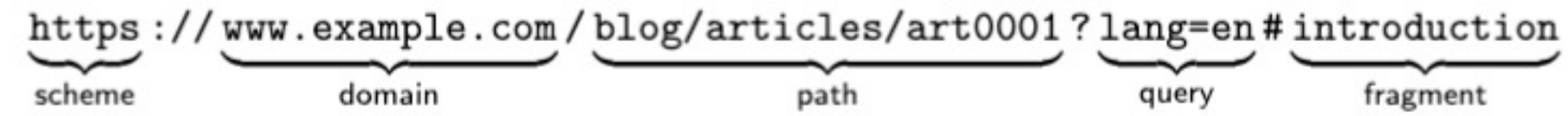
Anonymization for DGA detection

ML models have to be trained and can have drawbacks regarding data privacy

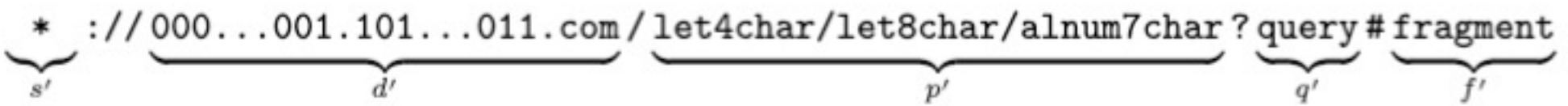
- Training requires a substantial amount of high-quality data
- Some (possibly sensitive) information about training data can be recovered from trained models

Possible solution:

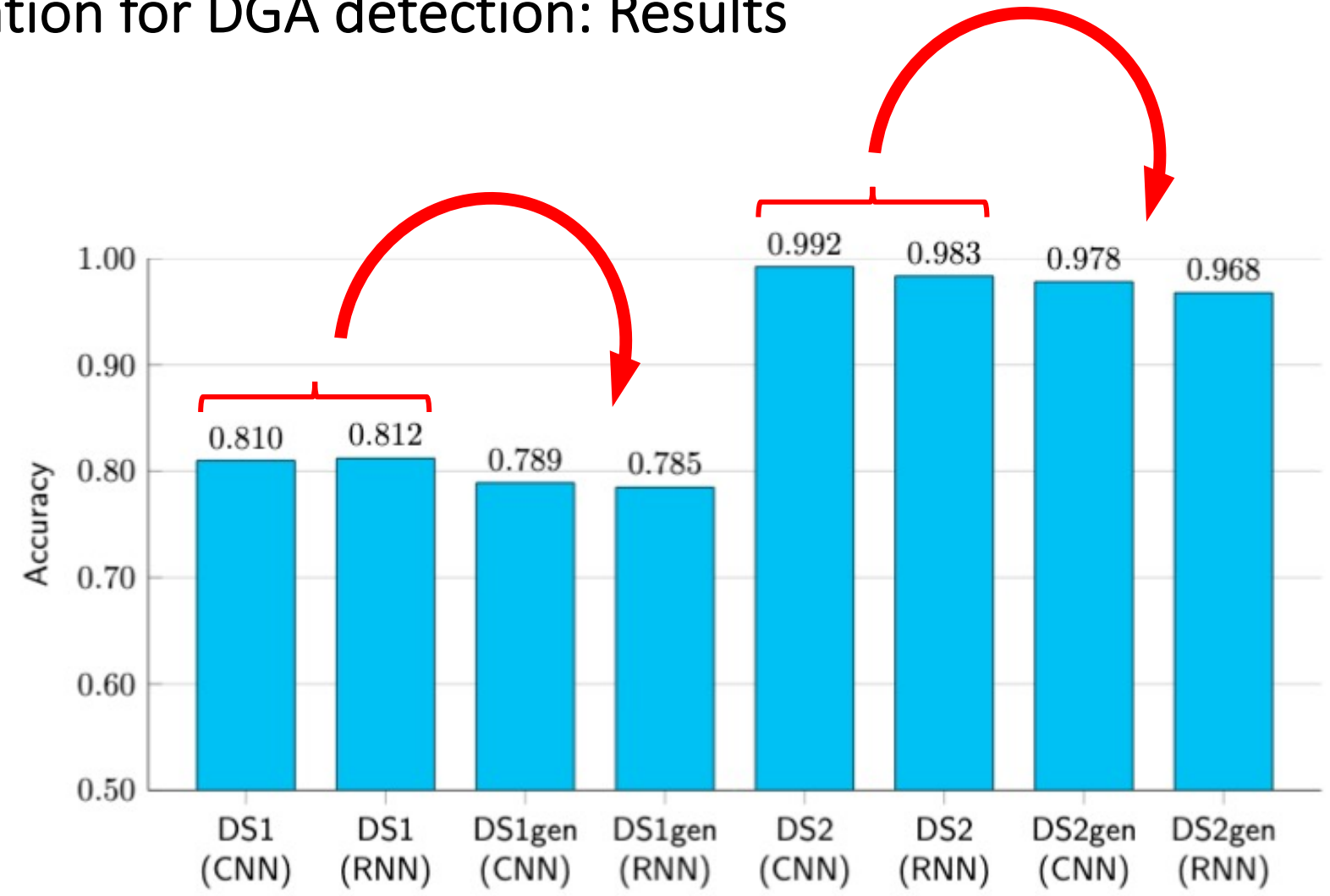
- Anonymize data before training models



Similarity preserving anonymization, ex. “Bloom filters”



Anonymization for DGA detection: Results



Nitz et. al, July 2020

Next steps for the project

Development of more local detection methods

- Host and application profiling based on netflow data
- Anomaly detection based on host profiles

Research on managing, automating and sharing response and recovery in machine readable way

- Playbooks, aligned with open standards (e.g. Open C2, IACD, …)
- Traffic light protocol to classify information to enable privacy when sharing

Research on federated machine learning approaches to overcome privacy and scalability drawbacks

Systematic evaluation of project KPIs in different organizations

- Technical measurements
- Surveys and collection of feedback

Pitch for participation in end user commitee

Pitch: Become part of the SAPPAN end user committee!

What we need your help with:

- Interview after demonstration of SAPPAN results and discussion of achievements

How much time it all take:

- 2 surveys + demonstration, 2 hours each

What you can expect in return:

- No cash
- Early access to results (papers)
- Early access to practical implementations (if open source)
- Access to new detectors as they are developped in showcases

What to do if you are interested:

- Send E-Mail to principal investigator benjamin.heitmann@fit.fraunhofer.de
- (Template on next page)

Pitch: Become part of the SAPPAN end user committee!
E-Mail Template

Dear Benjamin Heitmann,

I have received your request addressed to me to join the End User Committee of the SAPPAN project. Based on your introduction of the SAPPAN concept and the developed results, I express my interest in joining the End User Committee where I can contribute with my knowledge and expertise in assessment of the results.

Best,

EUC member


Thank
You!