Evaluation of a Multi-agent Anomaly-based Advanced Persistent Threat Detection Framework

Georgi Nikolov, Thibault Debatty, Wim Mees

Presenter: Georgi Nikolov

Affiliation: Cyber Defense Lab, Royal Military Academy, Belgium

Email: g.nikolov@cylab.be

Presenter Information - Georgi Nikolov

- Master Degree in Applied Informatics at the Vrije Universiteit Brussels (2015)
- Member of the Research Unit for Cyberdefense, Royal Military Academy Belgium (2016-2020)
- Lecturer training courses European Space Agency, Redu Belgium (2017-2020)
- GIAC Certified Forensic Analyst, Brussels Belgium (2018)

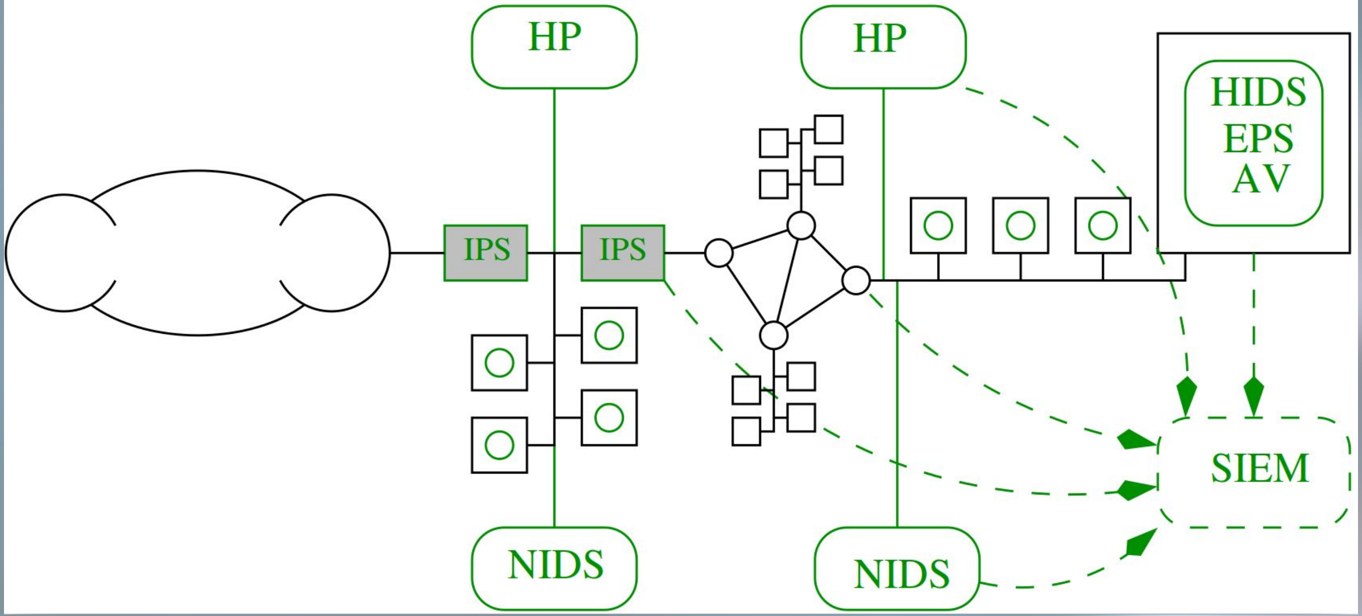
Context

Cybersecurity is constantly playing catch-up:

- Well organised and competent attackers
- New unknown zero-day vulnerability attacks
- Complex threat behavior
- Prolonged undetected activity over multiple hosts

Current Situation

"Information security continuous monitoring" (ISCM) program



Current Situation

*Examples of recent **A**dvanced **P**ersistent **T**hreat (APT) attacks*

1. Operation Socialist APT attack on Belgacom, 2013
2. Belgium targeted by the MiniDuke APT campaign, 2013
3. Pawn Storm APT attack against military, government and media organizations, 2015
4. StrongPity Waterhole Attack on Italian and Belgian Encryption users, 2016
5. APT28 (Fancy Bear) cyber espionage attack on Belgian and other European governments, 2018

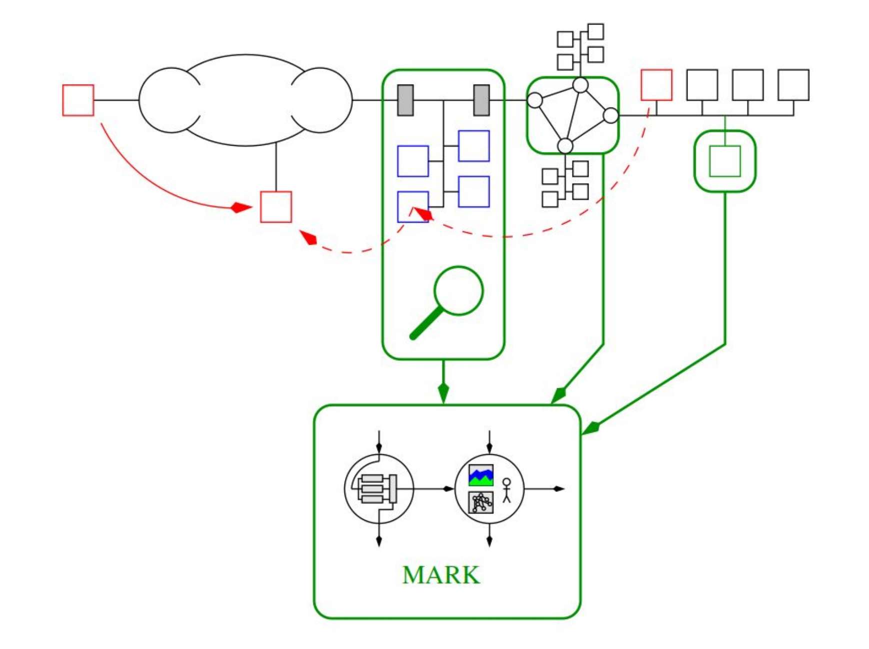
Proposed Solution

The **M**ulti-**a**gent **R**an**k**ing (MARK) Framework goals

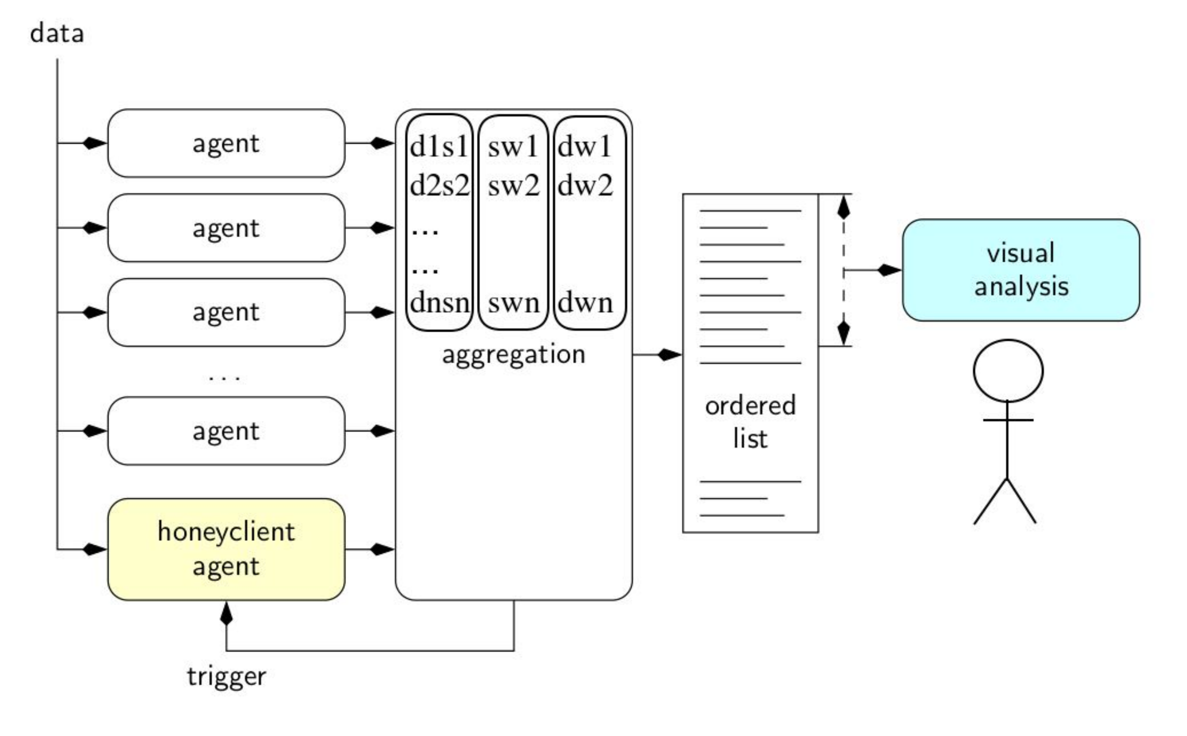
- ❖ Use of behavior-based detection heuristics
- ❖ Focus on detecting and analysing a set of APT characteristics
- ❖ Detect hidden **C**ommand & **C**ontrol (CnC) channels
- ❖ Evidence aggregation
- ❖ Evidence presentation for analysis by domain expert

Proposed Solution

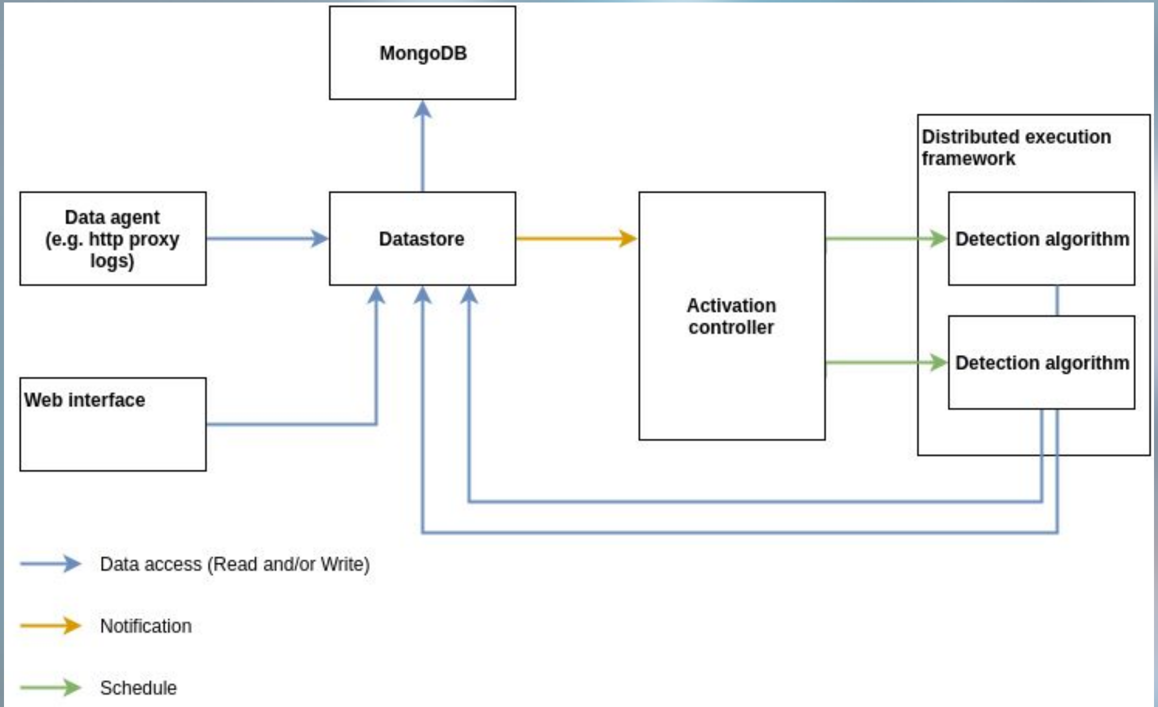
The Multi-agent Ranking Framework



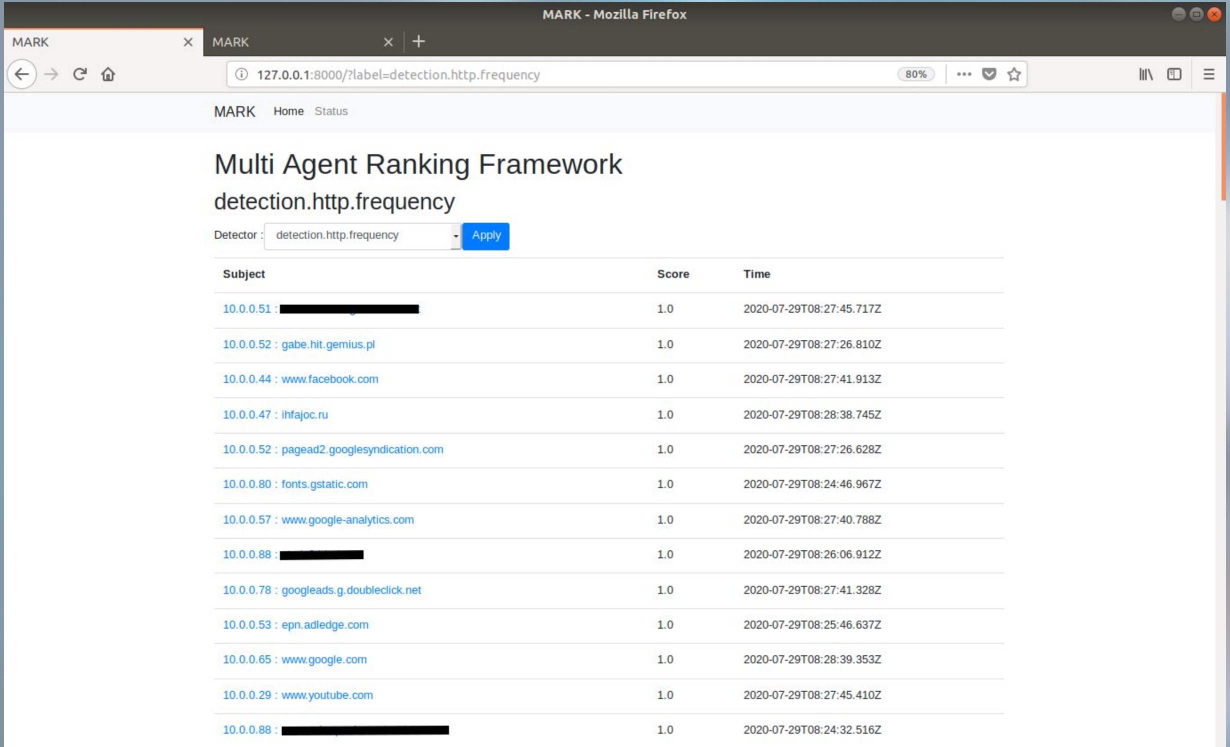
The MARK Framework Aggregation



The MARK Framework Implementation



The MARK Framework Visualization



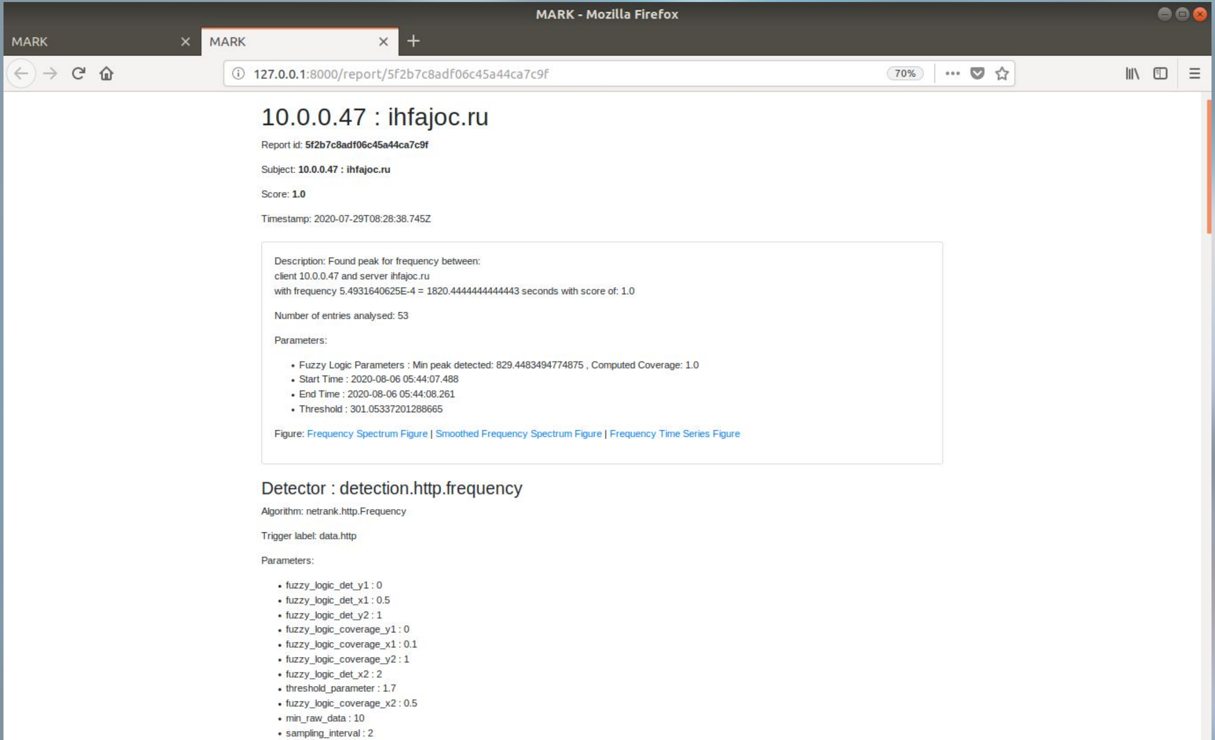
Multi Agent Ranking Framework

detection.http.frequency

Detector : detection.http.frequency

Subject	Score	Time
10.0.0.51 : [redacted]	1.0	2020-07-29T08:27:45.717Z
10.0.0.52 : gabe.hit.gemius.pl	1.0	2020-07-29T08:27:26.810Z
10.0.0.44 : www.facebook.com	1.0	2020-07-29T08:27:41.913Z
10.0.0.47 : ihfajoc.ru	1.0	2020-07-29T08:28:38.745Z
10.0.0.52 : pagead2.googlesyndication.com	1.0	2020-07-29T08:27:26.628Z
10.0.0.80 : fonts.gstatic.com	1.0	2020-07-29T08:24:46.967Z
10.0.0.57 : www.google-analytics.com	1.0	2020-07-29T08:27:40.788Z
10.0.0.88 : [redacted]	1.0	2020-07-29T08:26:06.912Z
10.0.0.78 : googleads.g.doubleclick.net	1.0	2020-07-29T08:27:41.328Z
10.0.0.53 : epn.adledge.com	1.0	2020-07-29T08:25:46.637Z
10.0.0.65 : www.google.com	1.0	2020-07-29T08:28:39.353Z
10.0.0.29 : www.youtube.com	1.0	2020-07-29T08:27:45.410Z
10.0.0.88 : [redacted]	1.0	2020-07-29T08:24:32.516Z

The MARK Framework Visualization



10.0.0.47 : ihfajoc.ru

Report id: **5f2b7c8adf06c45a44ca7c9f**

Subject: **10.0.0.47 : ihfajoc.ru**

Score: **1.0**

Timestamp: 2020-07-29T08:28:38.745Z

Description: Found peak for frequency between:
client 10.0.0.47 and server ihfajoc.ru
with frequency 5.4931640625E-4 = 1820.4444444444443 seconds with score of: 1.0

Number of entries analysed: 53

Parameters:

- Fuzzy Logic Parameters : Min peak detected: 829.4483494774875 , Computed Coverage: 1.0
- Start Time : 2020-08-06 05:44:07.488
- End Time : 2020-08-06 05:44:08.261
- Threshold : 301.05337201288665

Figure: Frequency Spectrum Figure | Smoothed Frequency Spectrum Figure | Frequency Time Series Figure

Detector : detection.http.frequency

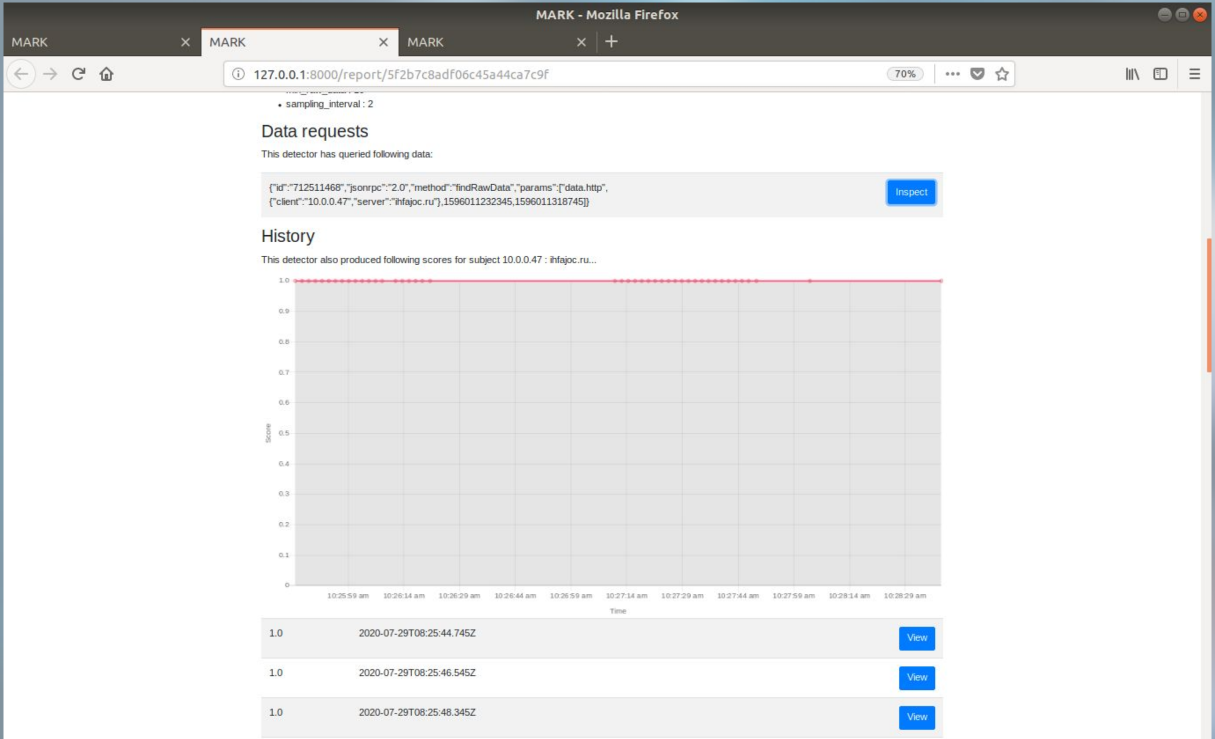
Algorithm: netrank.http.Frequency

Trigger label: data.http

Parameters:

- fuzzy_logic_det_y1 : 0
- fuzzy_logic_det_x1 : 0.5
- fuzzy_logic_det_y2 : 1
- fuzzy_logic_coverage_y1 : 0
- fuzzy_logic_coverage_x1 : 0.1
- fuzzy_logic_coverage_y2 : 1
- fuzzy_logic_det_x2 : 2
- threshold_parameter : 1.7
- fuzzy_logic_coverage_x2 : 0.5
- min_raw_data : 10
- sampling_interval : 2

The MARK Framework Visualization



- sampling_interval : 2

Data requests

This detector has queried following data:

```
{"id":"712511468","jsonrpc":"2.0","method":"findRawData","params":["data.http",
{"client":"10.0.0.47","server":"ihfajoc.ru"},1596011232345,1596011318745]}
```

History

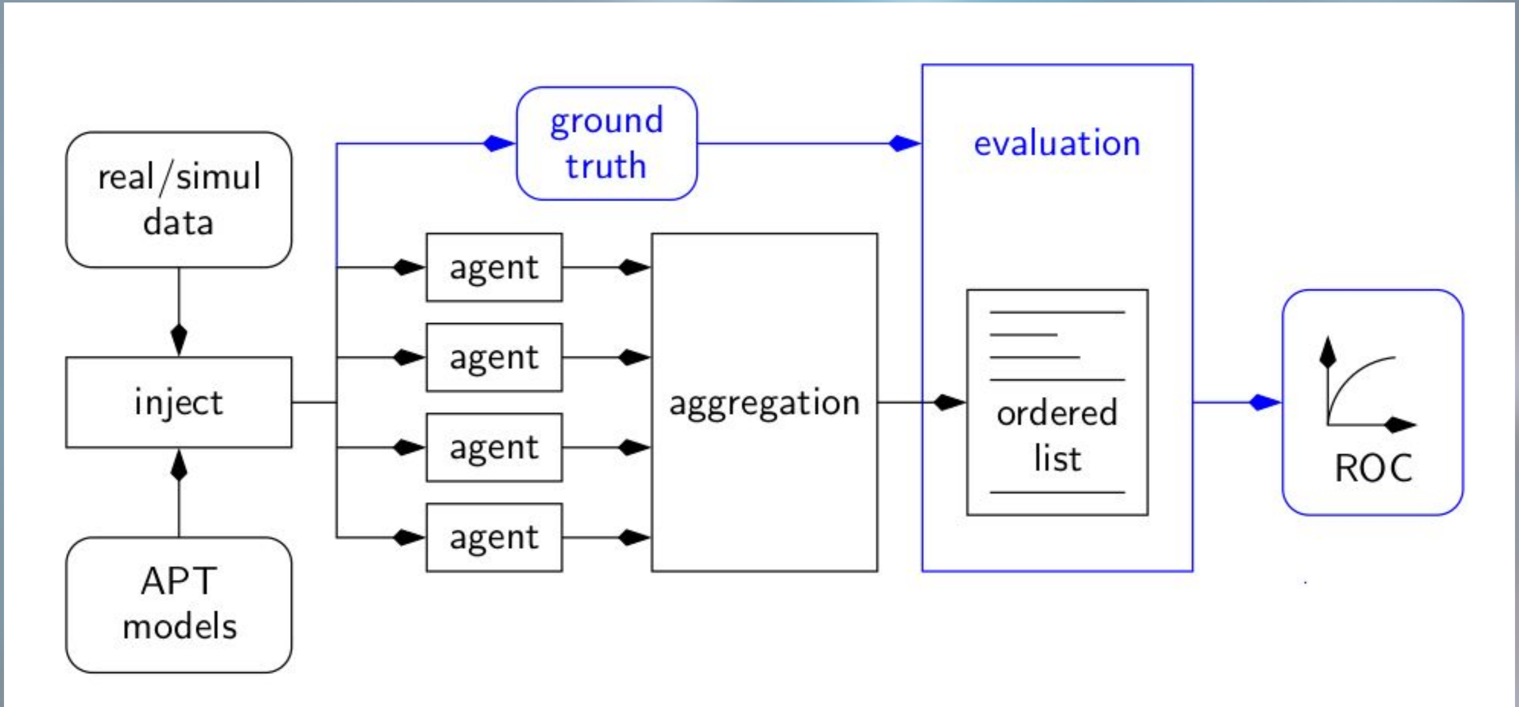
This detector also produced following scores for subject 10.0.0.47 : ihfajoc.ru...

1.0	2020-07-29T08:25:44.745Z	View
1.0	2020-07-29T08:25:46.545Z	View
1.0	2020-07-29T08:25:48.345Z	View

Evaluation and Benchmarking

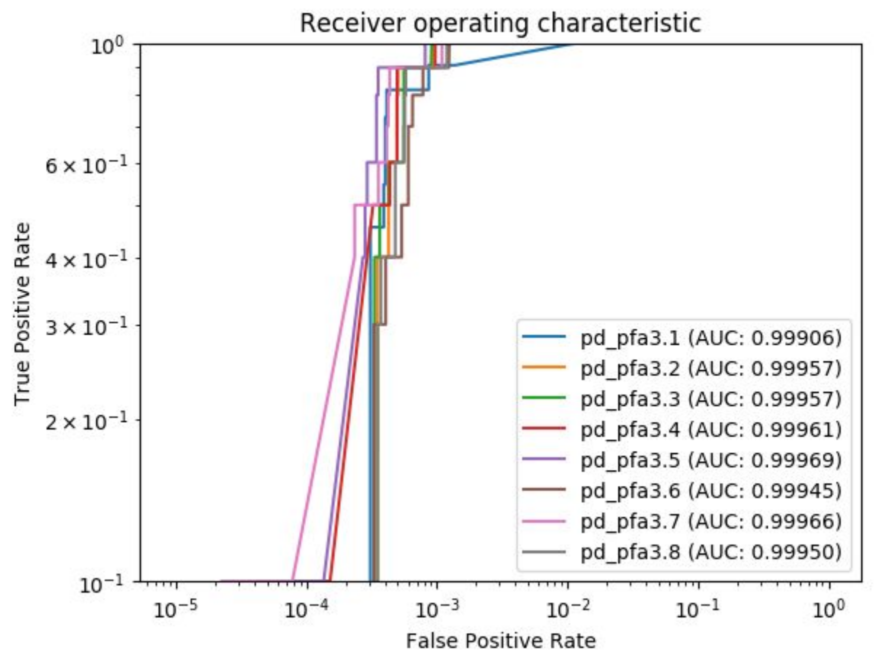
- In possession of real-world datasets for training and testing
  - Large Government Agency proxy logfiles
  - Enron SMTP dataset
- APT simulation and testing based on ground truth
- Estimate performance based on **R**eceiver **O**perating **C**haracteristic (ROC) curve and **A**rea **U**nder the **C**urve (AUC)

Evaluation and Benchmarking

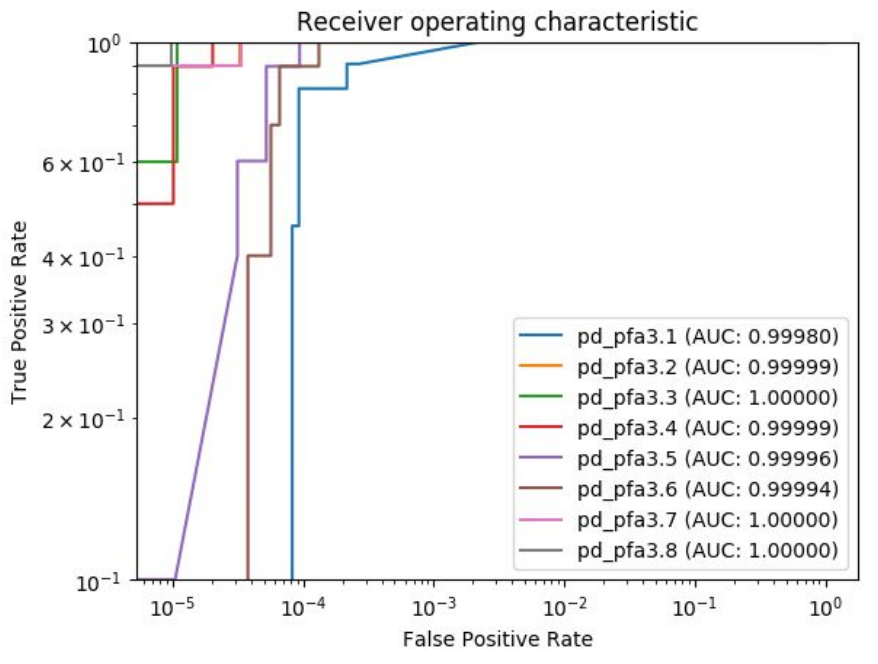


Evaluation Scenario 3

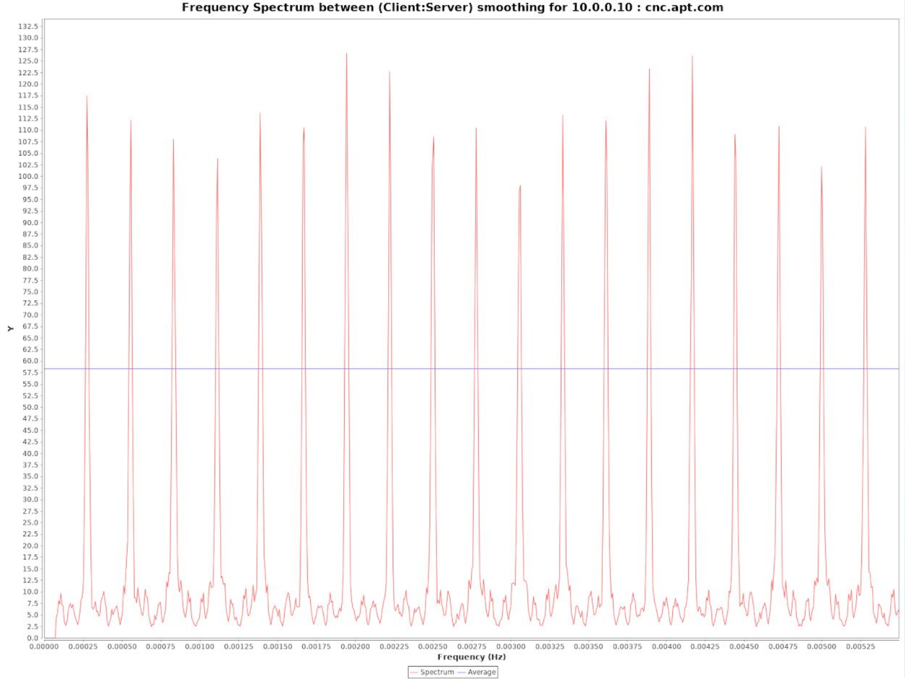
Results without Whitelisting



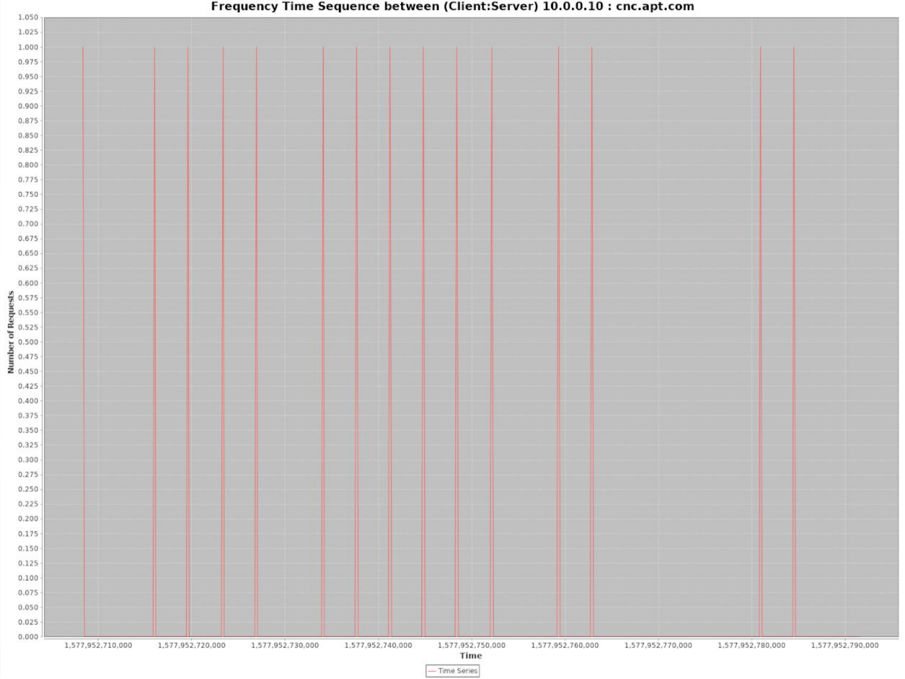
Results with Whitelisting



Detection Agent Examples (Frequency)

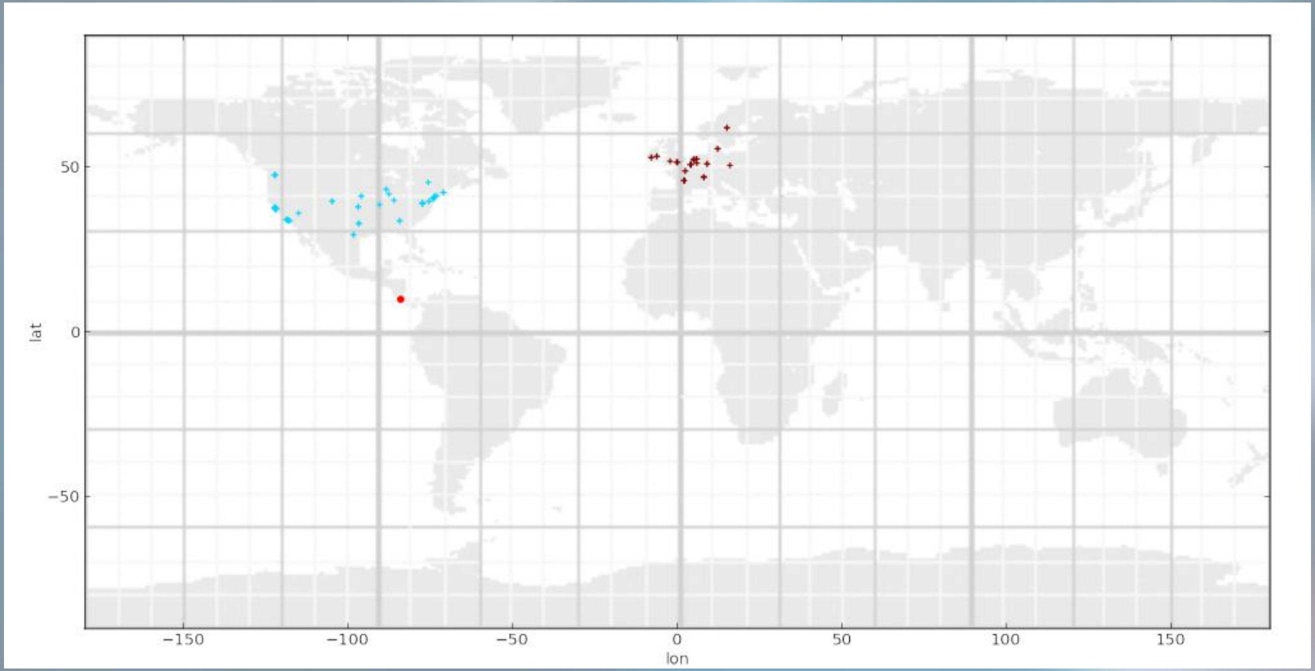


Frequency Spectrum between (Client:Server) smoothing for 10.0.0.10 : cnc.apt.com



Frequency Time Sequence between (Client:Server) 10.0.0.10 : cnc.apt.com

Detection Agent Examples (Geo-Outlier)



Future Work

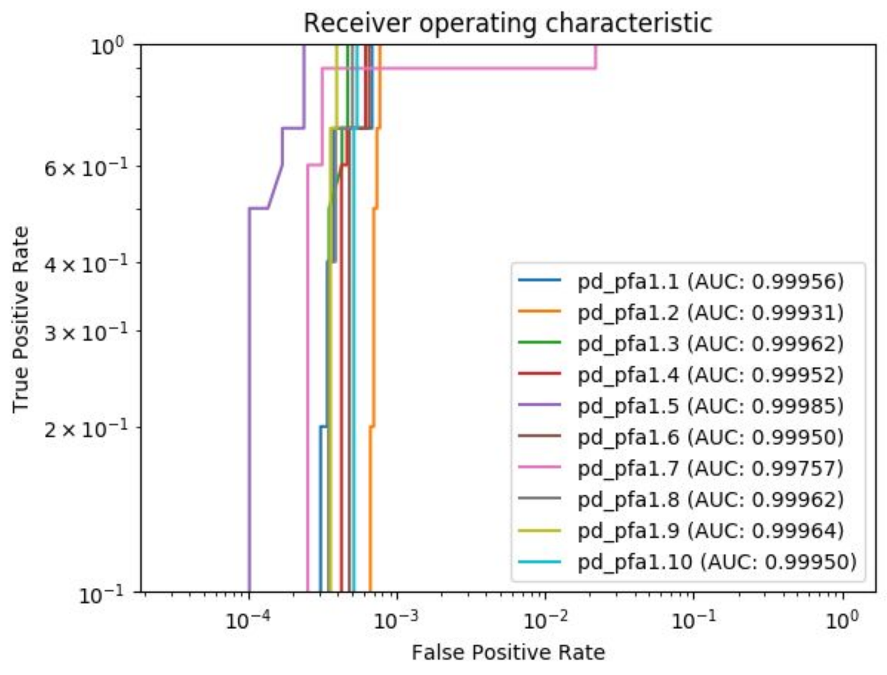
- Implementation of new detection techniques (for example using graph theory for APT detection)
- Incorporation of Weighted Ordered Weighted Averaging (WOWA)
- Using Machine Learning for parameter optimization
- Advanced visualizations following “Detection Through Visualization” methodology

Questions

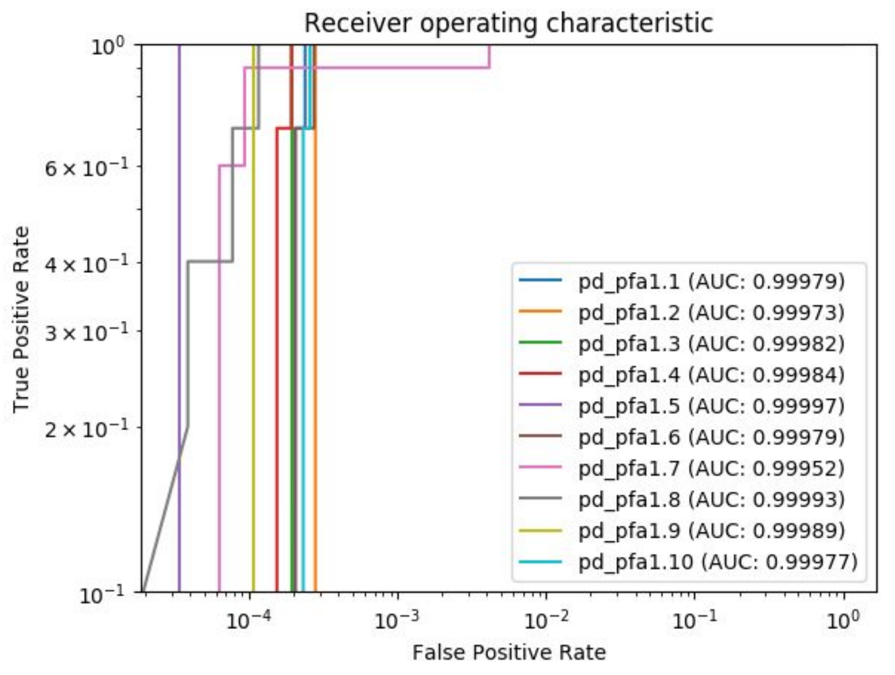
Thank you for your attention!

Evaluation Scenario 1 (Extra Slides)

Results without Whitelisting

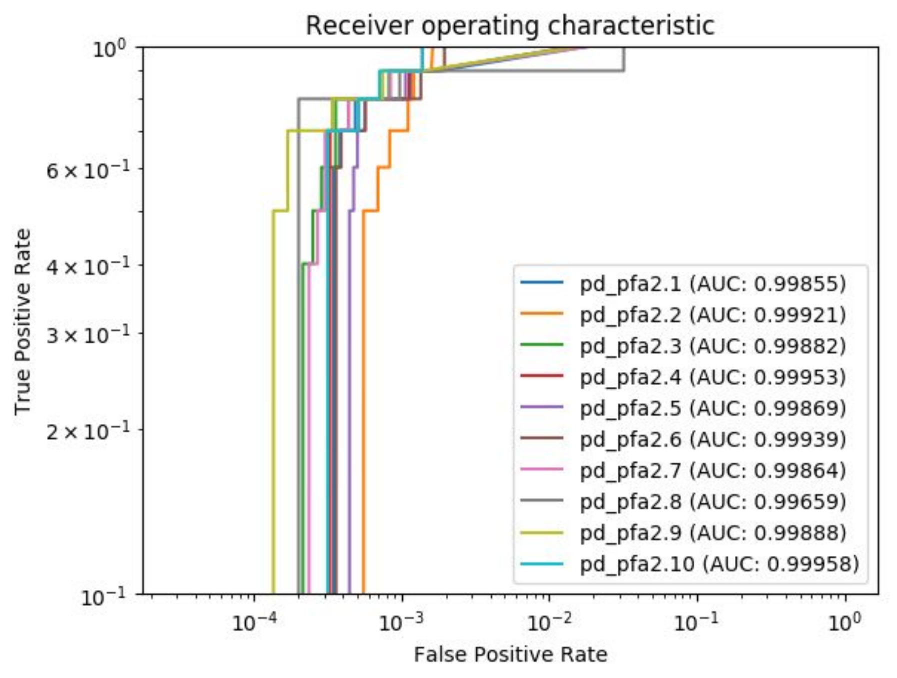


Results with Whitelisting

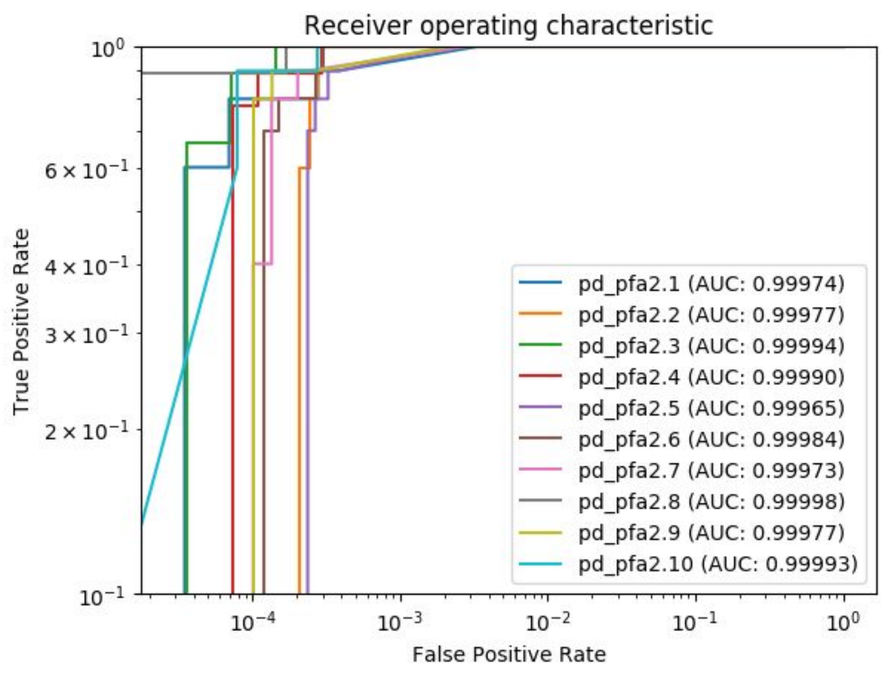


Evaluation Scenario 2 (Extra Slides)

Results without Whitelisting



Results with Whitelisting


Receiver operating characteristic
10^0
6×10^{-1}
4×10^{-1}
3×10^{-1}
2×10^{-1}
10^{-1}
True Positive Rate
10^{-4}
10^{-3}
10^{-2}
10^{-1}
10^0
False Positive Rate
pd_pfa2.1 (AUC: 0.99974)
pd_pfa2.2 (AUC: 0.99977)
pd_pfa2.3 (AUC: 0.99994)
pd_pfa2.4 (AUC: 0.99990)
pd_pfa2.5 (AUC: 0.99965)
pd_pfa2.6 (AUC: 0.99984)
pd_pfa2.7 (AUC: 0.99973)
pd_pfa2.8 (AUC: 0.99998)
pd_pfa2.9 (AUC: 0.99977)
pd_pfa2.10 (AUC: 0.99993)