An Approach to Detect and Prevent Cybercrime in Large Complex Networks

André Sørensen[1], Maxime Jérôme Remy[1], Nicolaj Kjettrup[1], Rasmi Vlad Mahmoud[1], Jens Myrup Pedersen[2]
[1]{asare14, mremy16, nkjett14, rmahmo17}@student.aau.dk,
[2]jens@es.aau.dk

AALBORG UNIVERSITY
DENMARK

Agenda

- Introduction
  - Contribution
- Methods
  - Prevention
  - Detection
- Evaluation
  - DNS Analysis
    - Individual Failure Rate
    - Individual Amount of Unique Failed Domain Request
  - Penetration Testing
- Conclusion
- Discussion

Introduction

- November **2016**: Center for Cybersecurity
  - **High threat**
  - Cyberespionage probably **already** occurring
- December **2017**: Danish Defence Intelligence Service
  - Cyberattack is the **highest threat** against Denmark
  - **Higher** threat than **terrorist attacks**

Contribution

- **Gap** in the research
  - **Companies**: Best practices
  - **Universities**: Specific methods
- Need for a **practical guide**
  - An Approach to **Detect and Prevent Cybercrime** in **Large Complex Networks**
  - Tested on **Aalborg University's network**
  - Validated according to **results** and **scalability**

Methods

- **Prevention**
  - **Penetration testing**
- **Detection**
  - Intelligent blacklist filter
  - Failure rate over time
  - **Individual failure rate**
  - **Individual amount of unique failed domain (UFD) request**

	DNS requests	Unique domains	Hosts	M. 1	M. 2	M. 3	M. 4
Four days of 2016	37.603.963	2.797.176	21.176	✓	✓	✓	✓
Five days of 2017	136.572.764	5.409.098	38.088	✗	✓	✓	✗
One day of 2017	23.965.859	1.224.536	21.841	✗	✗	✗	✓

Individual failure rate - 2016

- Noisy printers
- Hosts contacting **suspicious domains** such as
  - bhwcrqqwjx.bio.aau.dk
  - cxndvcquhte.aau.dk

Table: Selection of hosts with high failure rate.

Host ID	Requests	Failed Requests	Rate	Host Type
6	852	852	1	Printer
13610	2868	2868	1	Printer
7245	9013	9007	0.99	Printer
17207	9519	9510	0.99	Printer
17083	**1505**	**1452**	**0.96**	**Client**

Table: Selection of hosts with the high failure rate without printers

Host ID	Requests	Failed Requests	Rate
13588	216	216	1
17180	3057	3042	0.99
9266	43963	41921	0.95
5770	**71948**	**63562**	**0.88**
13468	**82629**	**72673**	**0.88**

Individual failure rate - 2017

- Possible to **detect hosts contacting suspicious domain** names
  - **Random domain** names such as
    - 5x5yaki.o897obvp.com
    - 7ocsnisnfpr19kmzug.d4i-322i53kzftsf.com
    - inldbcyjexs4f.9ibdnevxj7z799mnheo47yss.com
- Noisy machines in the network

Host ID	Requests	Failed Requests	Failure Rate	Cause
26237	**12911**	**12911**	**1**	**Random domains**
28449	1777	1777	1	Misspelled domains
28450	2906	2906	1	Misspelled domains
28451	9948	9948	1	Misspelled domains
31639	57411	57399	0.999	Misspelled domains
37599	**208471**	**204300**	**0.980**	**Random domains**
37266	**245194**	**232186**	**0.947**	**Random domains**

Individual Amount of UFD Request - 2016

- **4 days** of data
  - 974 hosts with least at 100 UFD
  - **Suspicious domains**
    - adkcuyaxbroqoaf.aau.dk
    - ddxdpdhmelunua.nano.aau.dk

Table: The top 7 hosts with most UFD

Host ID	UFD
14879	**9490**
17128	**8162**
10152	7788
10166	6646
13399	5668
9981	3793
16372	3435

Individual Amount of UFD Request - 2017

- The **hosts with the highest UFD** are all **contacting random subdomains** (with one exception)
- **Similar to** data set from **2016** but only analyzed for **1 day**

Table: The top 7 hosts with most UFD

Host ID	UFD	Cause
10549	4747	Our computer
17171	**2690**	**Random subdomains**
5483	**1873**	**Random subdomains**
10190	1739	Random subdomains
13898	1381	Random subdomains
15354	1256	Random subdomains
8586	872	Random subdomains

AALBORG UNIVERSITY
DENMARK

Penetration Testing – Vulnerability Scanning

- **1071 host scanned** in 18 h and 21 min.
  - **8982 vulnerabilities** found (230 unique)
  - **684** hosts with **at least one vulnerability**
- Vulnerabilities assessed using the metric **CVSS v3.0**
  - Metrics based on **exploitability** and **impacts** of the exploit
  - Critical: **Execute** arbitrary **code** or **unsupported** version
  - High: **Denial** of service
  - Medium: **Man in the middle** attack
  - Low: **Unencrypted** communication

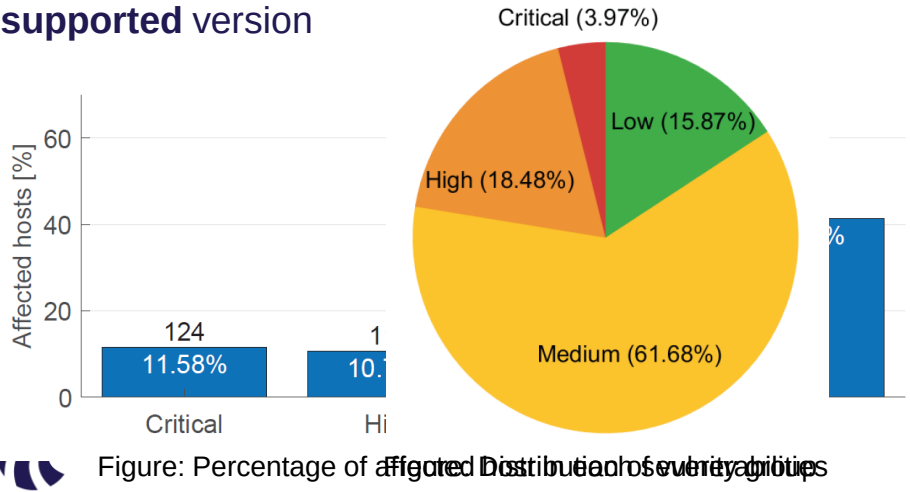

Figure: Percentage of affected hosts and distribution of severity groups

Discussion

- **Penetration Testing**
  - Problems
    - Can cause **harm** and/or **disturbances** to the scanned systems
    - **Lack scalability**.
  - Gains
    - Only method able to assess and provide an overview of a network's security.
- **DNS Analysis**
  - Random subnet attacks
  - Algorithm to detect random domain names
  - Improve efficiency and automation

Conclusion

- **Results**
  - ✓ Penetration testing
  - ✓ Intelligent blacklist filter
  - X Failure rate over time
  - ✓ Individual failure rate
  - ✓ Individual amount of unique failed domain requests

- **Scalability**
  - X Penetration testing
    - ✓ Vulnerability scanning
  - ✓ Intelligent blacklist filter
  - ✓ Failure rate over time
  - ✓ Individual failure rate
  - ✓ Individual amount of unique failed domain requests