



UNIVERSITEIT VAN AMSTERDAM

T-Mobile

T-Systems



Research Project 1

**Securing an outsourced network:  
Detecting and preventing malware infections**

# Agenda

---

- Introduction
- Research
- Theory
- Hardware
- Software
- Architecture
- HTTP request
- Checks
- Demo
- Test
- Summary

Dennis Cortjens

Tarik El Yassem

Sheets: 16

Duration: 25 minutes

Questions: after presentation

# Introduction

---

- T-Mobile
- Outsourced IT Service Management
- Bring-your-own-device

T-Mobile  
vs  
T-Systems



# Research

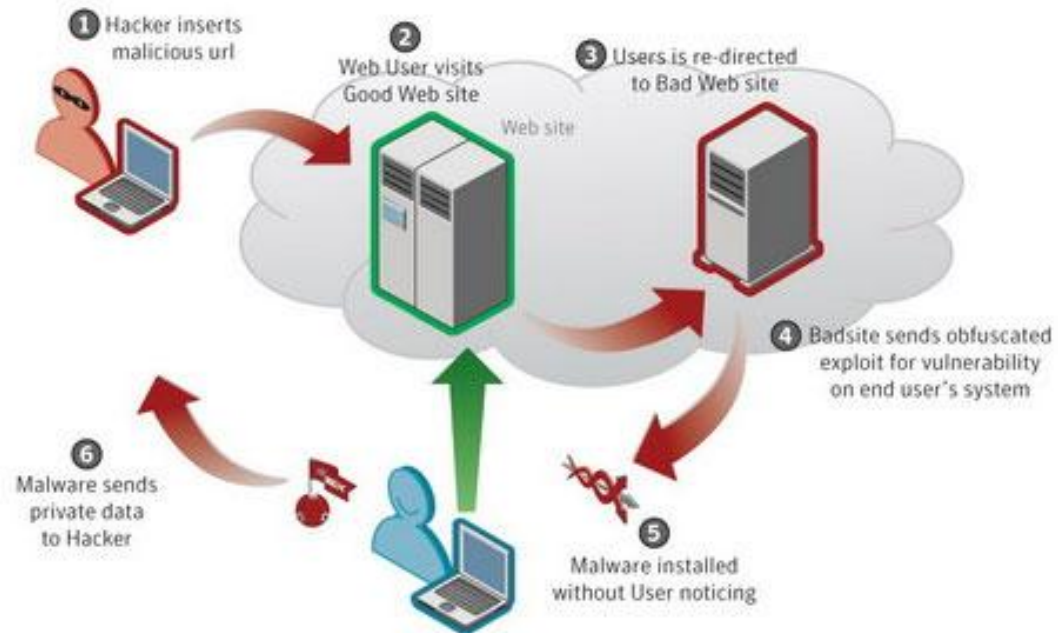
---

*“ How could malware infection attempts be detected and prevented from within the IT infrastructure of the business that has outsourced IT service management or that allows 'bring your own device'? ”*

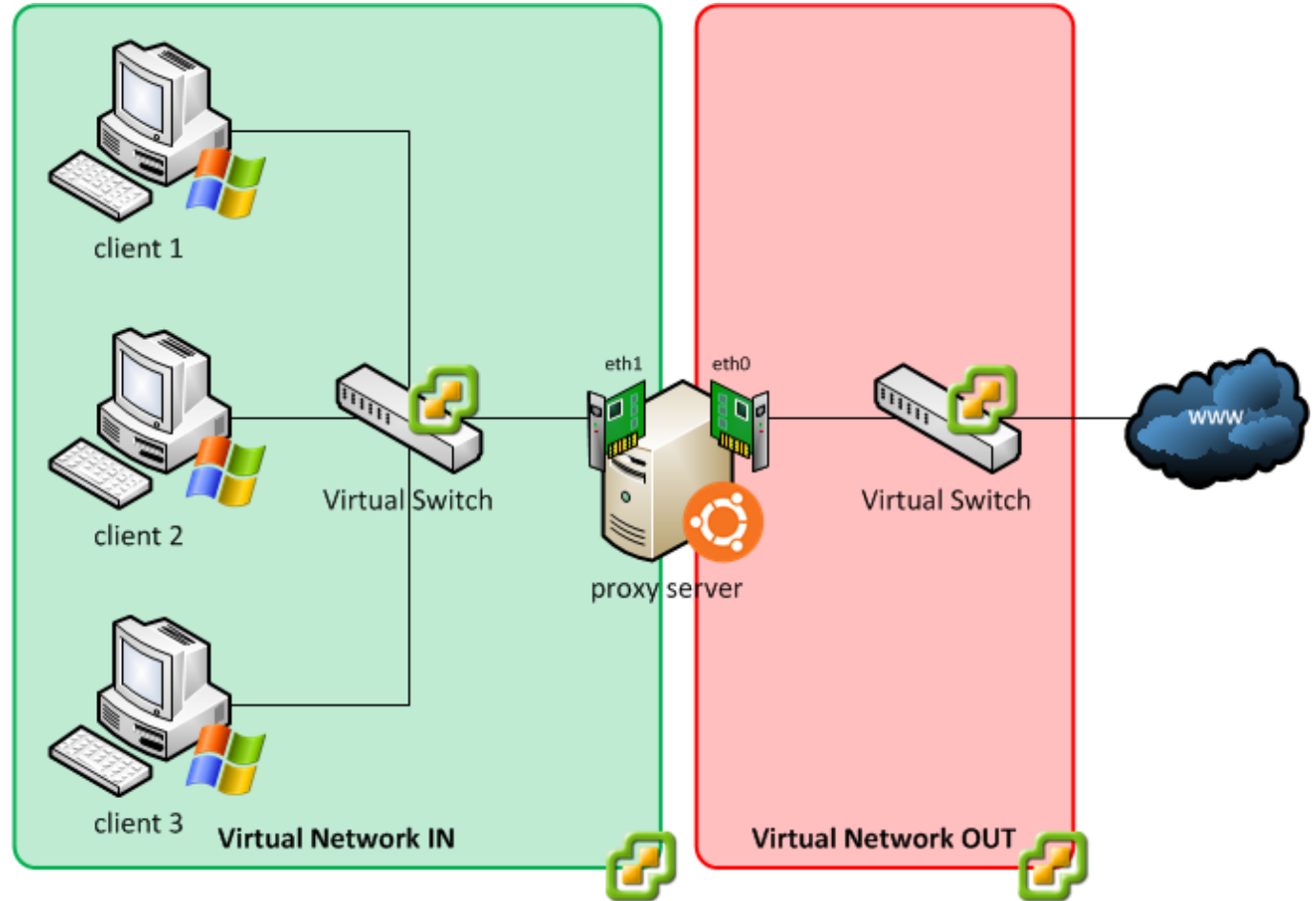
- other research (OS3):
  - Detecting the ghost in the browser:  
Real time detection of drive-by infections
  - HTTP Session Identification

# Theory

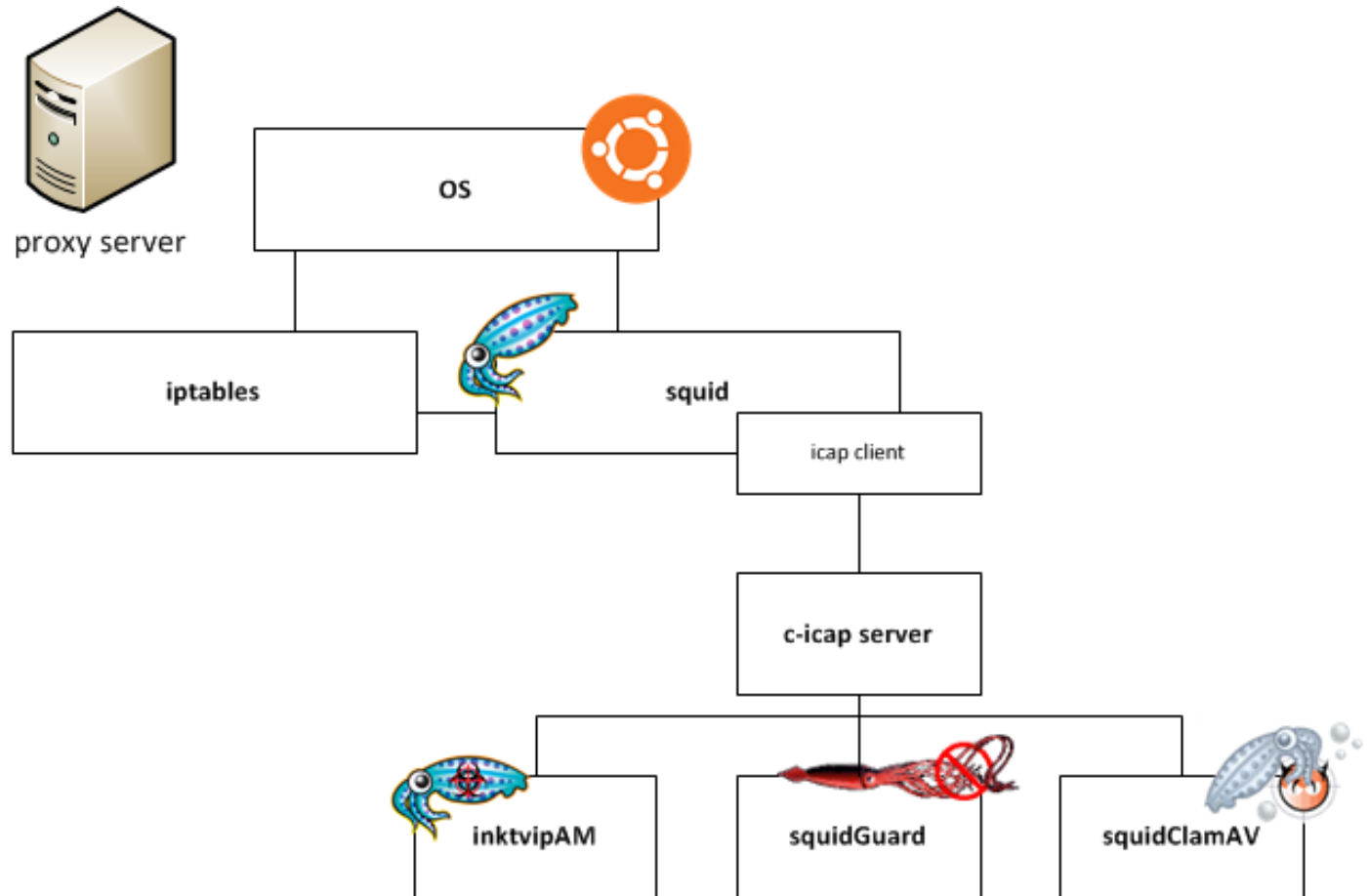
- Malware
- Drive-by downloads



# Hardware

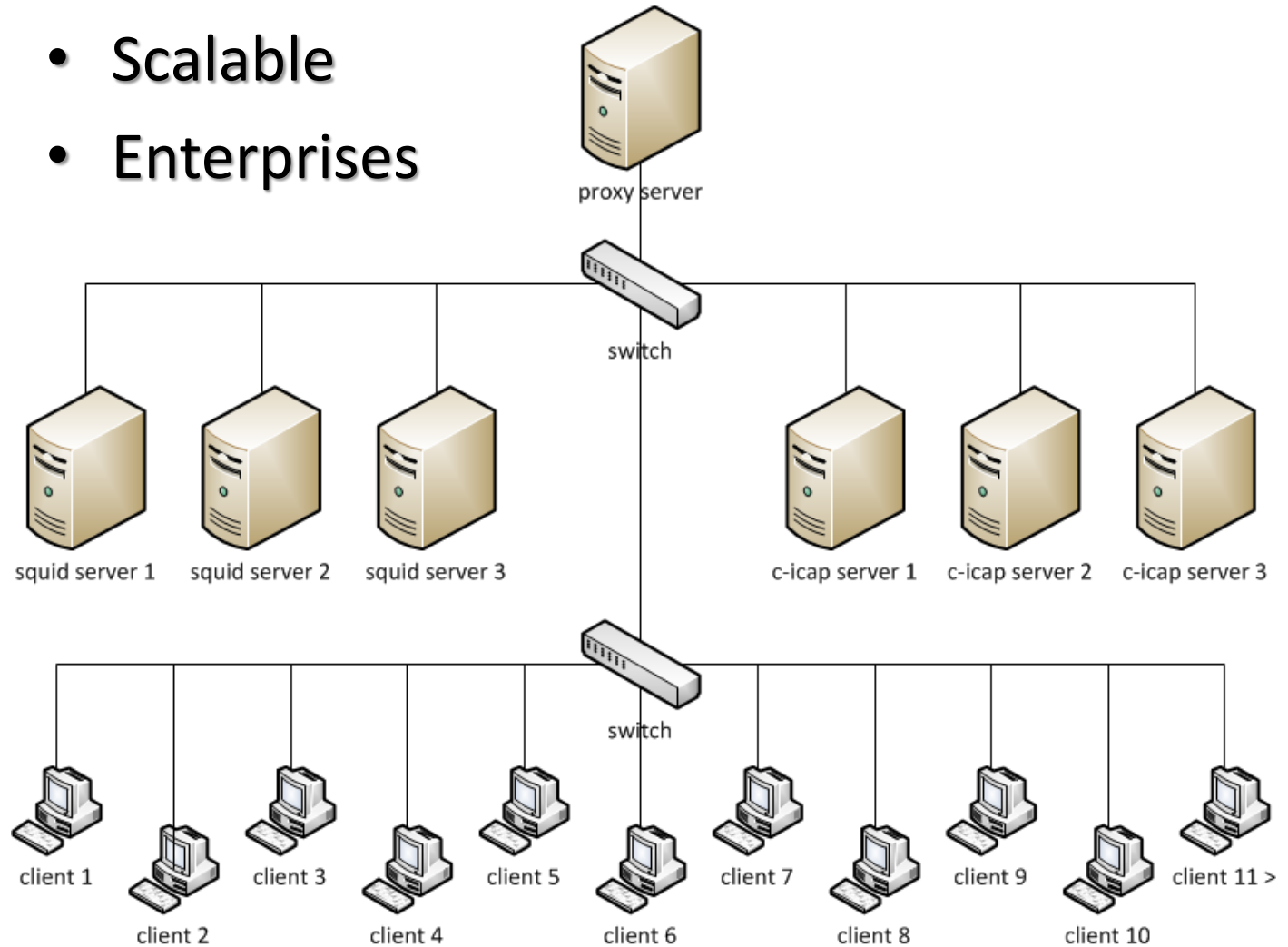


# Software



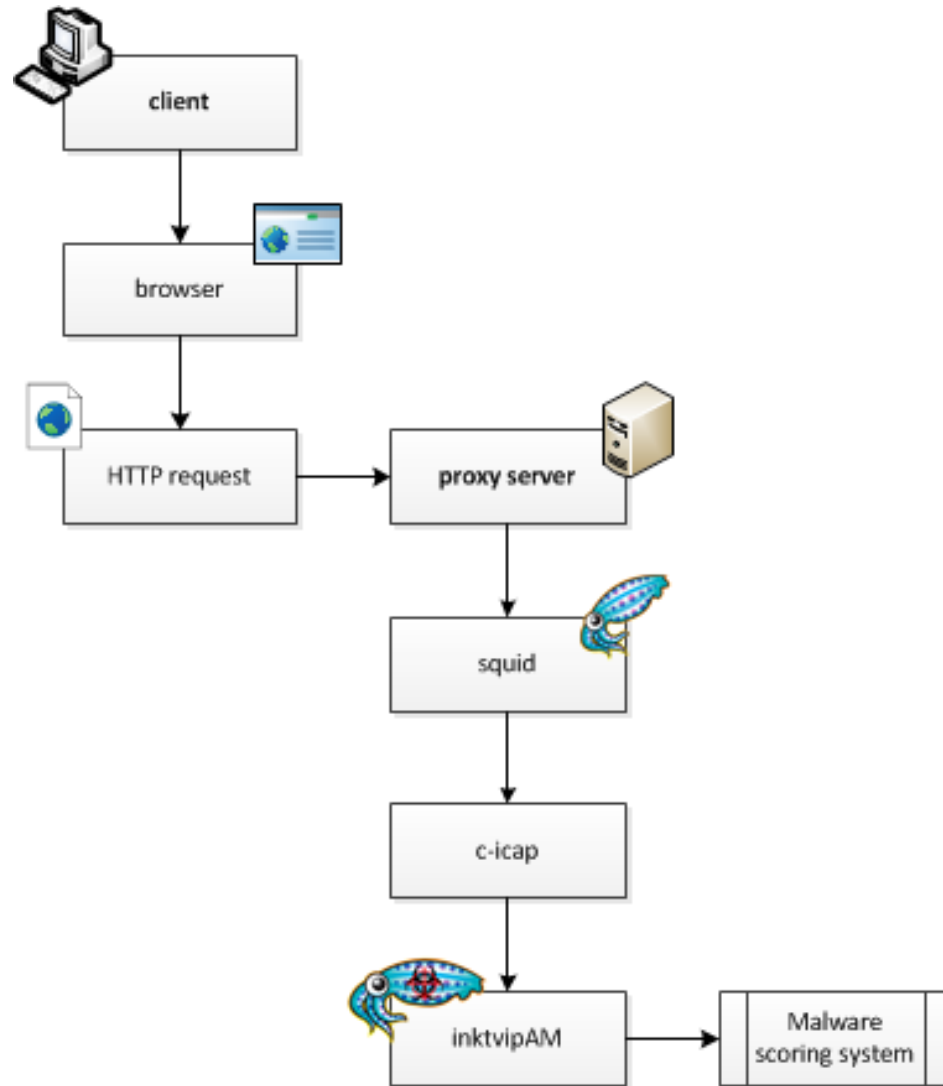
# Architecture

- Scalable
- Enterprises





# HTTP request

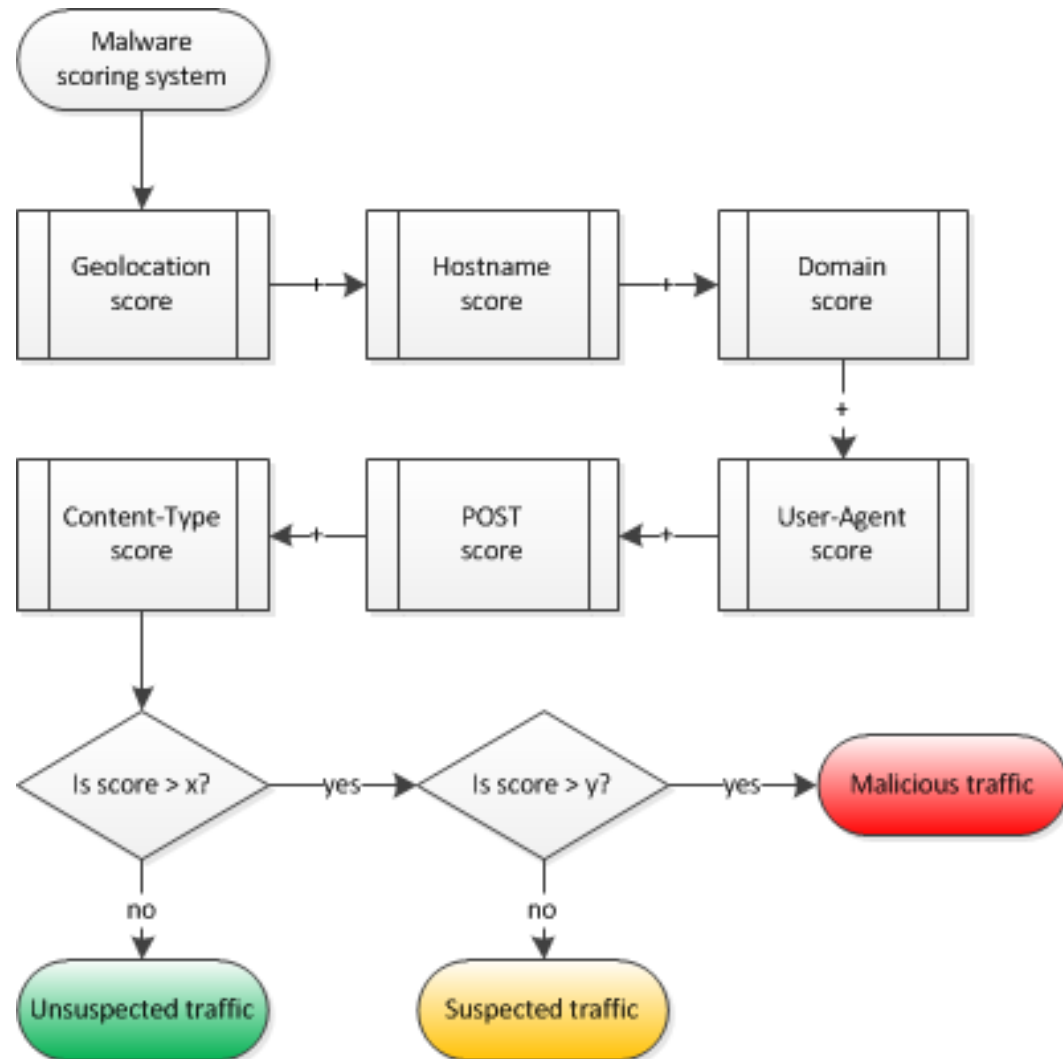


# Checks

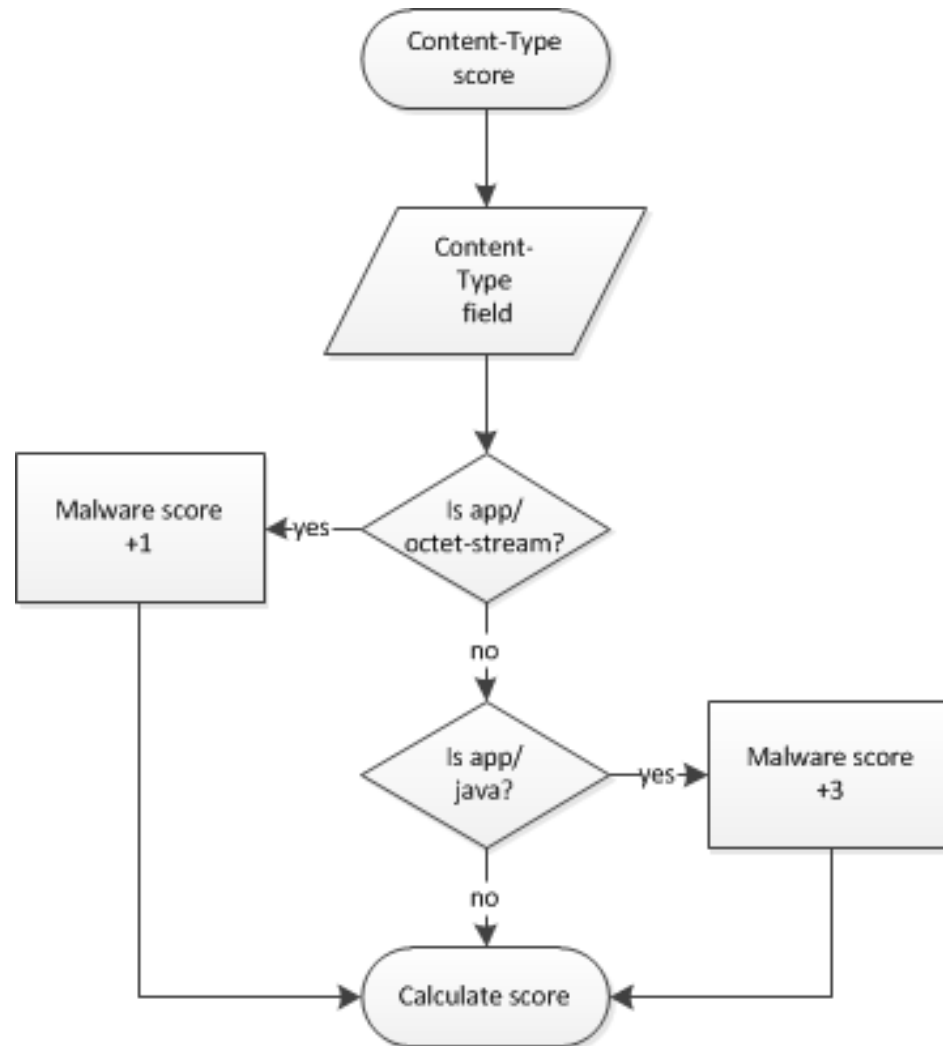
---

- ✗ TCP ports
- ✓ Geolocation
- ✓ Hostname
- ✓ Domain
- ✓ User-Agent
- ✓ POST
- ✓ Content-Type

# Scoring system



# Content-Type



# Demo

---

- [www.facebook.com](http://www.facebook.com)
- [www.piratebay.org](http://www.piratebay.org)
- [137.254.16.66/nl/download/installed.jsp](http://137.254.16.66/nl/download/installed.jsp)



# facebook

Email  Password

Keep me logged in [Forgot](#)

```

root@tmnl-proxy: ~
=====
DEBUG HTTP Hostname: www.facebook.com
DEBUG HTTP Hostname is unsuspected! MALWARE SCORE: 0
DEBUG HTTP URL is: www.facebook.com
DEBUG HTTP URL is not an IP address! MALWARE SCORE: 0
DEBUG HTTP User-Agent is: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET
50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
DEBUG HTTP User-Agent render engine 'Mozilla/4.0' is whitelisted! MALWARE Score: 0
DEBUG HTTP User-Agent browser 'compatible; MSIE 6.0;' is whitelisted! MALWARE SCORE: 0
DEBUG HTTP User-Agent is unsuspected! MALWARE SCORE: 0
DEBUG HTTP Content-Length is empty! MALWARE SCORE: 1
DEBUG HTTP Content-Type is: text/html; charset=utf-8
DEBUG HTTP Content-Type is unsuspected! MALWARE SCORE: 0
DEBUG unsuspected traffic! Allowing traffic! TOTAL MALWARE SCORE: 1
=====

```

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Folders Favorites

Address <http://thepiratebay.se/> Go Links



```
root@tmnl-proxy: ~  
=====  
DEBUG HTTP Hostname: 194.71.107.15  
DEBUG HTTP Hostname is unsuspected! MALWARE SCORE: 0  
DEBUG HTTP URL is: 194.71.107.15  
DEBUG HTTP URL is an IP address! MALWARE SCORE: 2  
DEBUG HTTP User-Agent is: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET  
50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
DEBUG HTTP User-Agent render engine 'Mozilla/4.0' is whitelisted! MALWARE Score: 0  
DEBUG HTTP User-Agent browser 'compatible; MSIE 6.0;' is whitelisted! MALWARE SCORE: 0  
DEBUG HTTP User-Agent is unsuspected! MALWARE SCORE: 0  
DEBUG HTTP Content-Length is: 26  
DEBUG HTTP body size is: 26  
DEBUG HTTP Content-Length is unsuspected! MALWARE SCORE: 0  
DEBUG HTTP Content-Type is: text/html  
DEBUG HTTP Content-Type is unsuspected! MALWARE SCORE: 0  
DEBUG unsuspected traffic! Allowing traffic! TOTAL MALWARE SCORE: 2  
=====
```



```

root@tmnl-proxy: ~
=====
DEBUG HTTP Hostname: 137.254.16.66
DEBUG HTTP Hostname is unsuspected! MALWARE SCORE: 0
DEBUG HTTP URL is: 137.254.16.66
DEBUG HTTP URL is an IP address! MALWARE SCORE: 2
DEBUG HTTP User-Agent is: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_20
DEBUG HTTP User-Agent render engine 'Mozilla/4.0' is whitelisted! MALWARE Score: 0
DEBUG HTTP User-Agent is unsuspected! MALWARE SCORE: 0
DEBUG HTTP Content-Length is: 1449
DEBUG HTTP body size is: 1449
DEBUG HTTP Content-Length is unsuspected! MALWARE SCORE: 0
DEBUG HTTP Content-Type is: application/java-vm
DEBUG HTTP Content-Type contains 'application/java'! MALWARE SCORE: 3
DEBUG malicious traffic! Blocking traffic! TOTAL MALWARE SCORE: 5
=====


```

installatie.

Hulpbronnen

- » [Wat is Java?](#)
- » [Foutmeldingen](#)
- » [Oudere versies](#)

[verwijderen](#)

 Error. Click for details





# Test

|   | H | D | UA | P | CT | ALLOW | BLOCK |
|---|---|---|----|---|----|-------|-------|
| google.nl                               | 0 | 0 | 0  | 0 | 0  | X     |       |
| google.com                              | 0 | 0 | 0  | 0 | 0  | X     |       |
| facebook.com                            | 0 | 0 | 0  | 1 | 0  | X     |       |
| wikipedia.org                           | 0 | 0 | 0  | 0 | 0  | X     |       |
| nu.nl                                   | 0 | 0 | 0  | 1 | 0  | X     |       |
| ing.nl                                  | 0 | 0 | 0  | 0 | 0  | X     |       |
| t.co                                    | 0 | 0 | 0  | 0 | 0  | X     |       |
| tweakers.net                            | 0 | 0 | 0  | 0 | 0  | X     |       |
| piratebay.org                           | 0 | 0 | 0  | 1 | 0  | X     |       |
| powned.tv                               | 0 | 0 | 0  | 0 | 0  | X     |       |
| 69.171.242.53                           | 0 | 0 | 0  | 1 | 0  | X     |       |
| 194.71.107.15                           | 0 | 2 | 0  | 0 | 0  | X     |       |
| 137.254.16.66/nl/download/installed.jsp | 0 | 2 | 0  | 0 | 3  |       | X     |

- testing on a larger scale is required
- further balancing is needed

# Summary

---

*“ Our **concept** is a practical way of **trying** to detect and prevent drive-by malware infections by analysing HTTP traffic patterns. “*

- HTTP request header data
- Improved known methods/checks
- Implemented working concept
- A scalable enterprise solution
- An open platform for further research

# Thank you for your attention...

