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

Sheets: 16
Duration: 25 minutes
Questions: after presentation
Introduction

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

T-Mobile vs T-Systems
“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
• Malware  
• Drive-by downloads
Hardware

Diagram showing a network setup with clients and virtual switches.
• **Scalable**
• **Enterprises**

![Architecture Diagram](image-url)
HTTP request

1. Client
2. Browser
3. HTTP request
4. Proxy server
5. Squid
6. c-icap
7. InktvIPAM
8. Malware scoring system
Checks

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

Malware scoring system

- Geolocation score
- Hostname score
- Domain score

- Content-Type score
- POST score
- User-Agent score

Is score > x?
- yes
- no

Is score > y?
- yes
- no

- Malicious traffic
- Unsuspected traffic
- Suspected traffic
Content-Type

1. Calculate Content-Type score
2. Check Content-Type field
3. If app/octet-stream? Yes → Malware score +1
4. No →
   a. If app/java? Yes → Malware score +3
   b. No → Calculate score
• www.facebook.com
• www.piratebay.org
• 137.254.16.66/nl/download/installed.jsp
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
TCP 443

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

installatie.

Error. Click for details
• testing on a larger scale is required
• further balancing is needed
“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...

...another day at the support group for computers with malware...