



**Luke Jennings**

Internal Network Access  
Via Externally Launched  
Browser Attacks

Current Advanced  
Techniques

**8<sup>th</sup> September 2011**



# Outline

- Introduction
- Perimeter Security Model
- Modern Reality
- The Compromised Workstation
- The Attack Vector
- Live Demo
- Defence
- Conclusion



# Introduction

- Internal networks are **not secure**
- Internal threat agents **do exist**
- External attackers can **breach your perimeter**



# Outline

- Introduction
- Perimeter Security Model
- Modern Reality
- The Compromised Workstation
- The Attack Vector
- Live Demo
- Defence
- Conclusion



# Perimeter Security Model





# Perimeter Security Model

- Not Realistic
- Modern Working Practices Differ Significantly
- Internal Threats Do Exist
- No Defence in Depth



# Outline

- Introduction
- Perimeter Security Model
- **Modern Reality**
- The Compromised Workstation
- The Attack Vector
- Live Demo
- Defence
- Conclusion



# Modern Reality

- No Strict Perimeter
- Mobile Computing
- “Everything over HTTP”
- Poor Physical Security Procedures
- Third Parties/Contractors
- USB Media



# Outline

- Introduction
- Perimeter Security Model
- Modern Reality
- **The Compromised Workstation**
- The Attack Vector
- Live Demo
- Defence
- Conclusion



# The Compromised Workstation

- Conventional Server Attacks
  - Small surface area
  - Hardened Builds
  - DMZs
- Workstations - Client Side Attacks
  - HUGE surface area
  - No DMZ
  - Many 0-days
  - Bad Patching
  - Anti-Virus Difficult



# The Compromised Workstation

- Ok, so a couple of my workstations get compromised....so what?
- A single compromised desktop can...
  - Allow full VPN-like access
  - Expose your weak internal network to the internet
  - Be controlled via proxies, DNS, direct connections etc
- And what if the compromised workstation is used by an administrator?



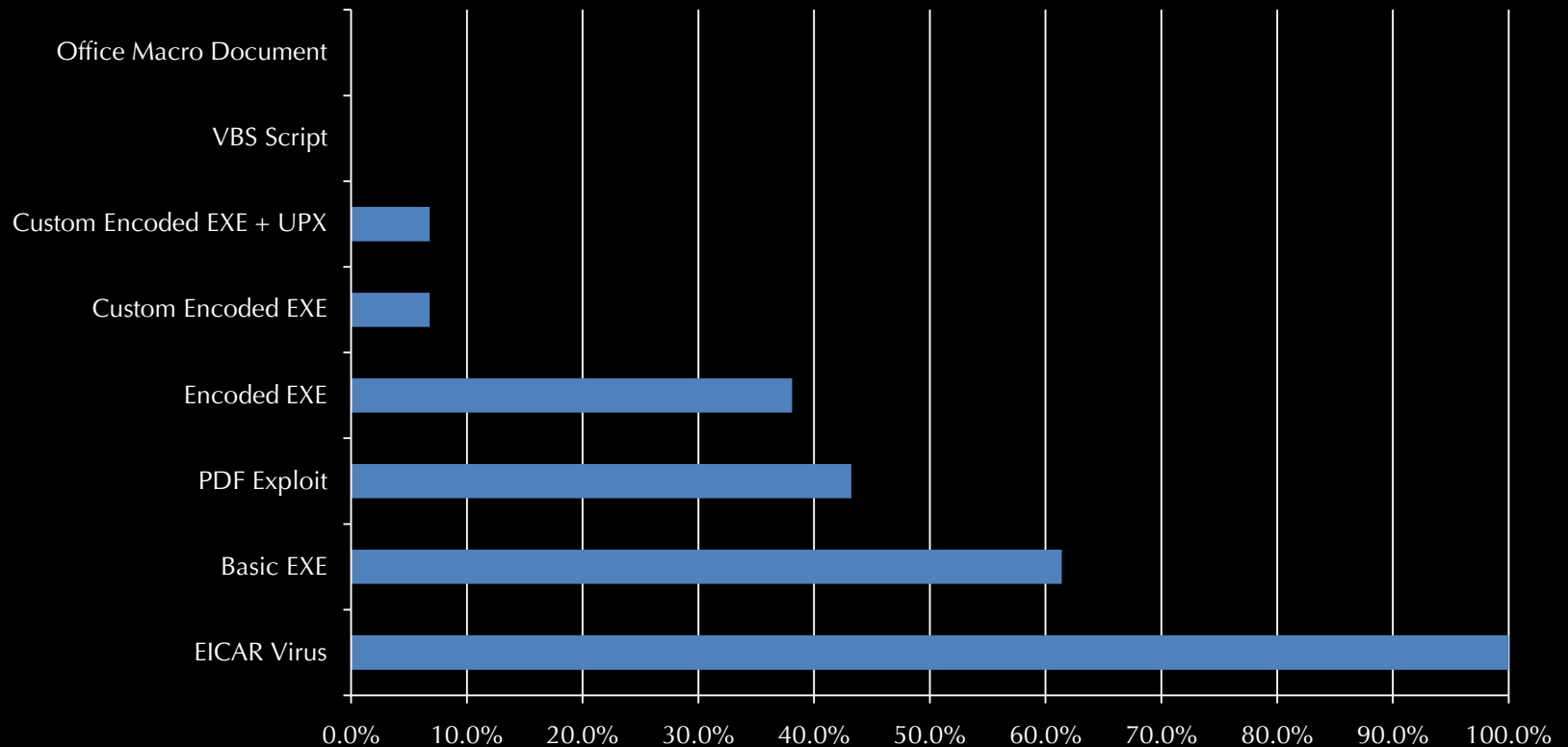
# The Compromised Workstation

- Exploitable Software
  - Web Browsers
  - Microsoft Office
  - Java, Flash and many more
- Delivery Mechanisms
  - Web Browsing
  - Email
  - Removable Media
  - Social Engineering

# The Compromised Workstation

- But my Anti-Virus will save me....right?

Virus Total Detection Rate





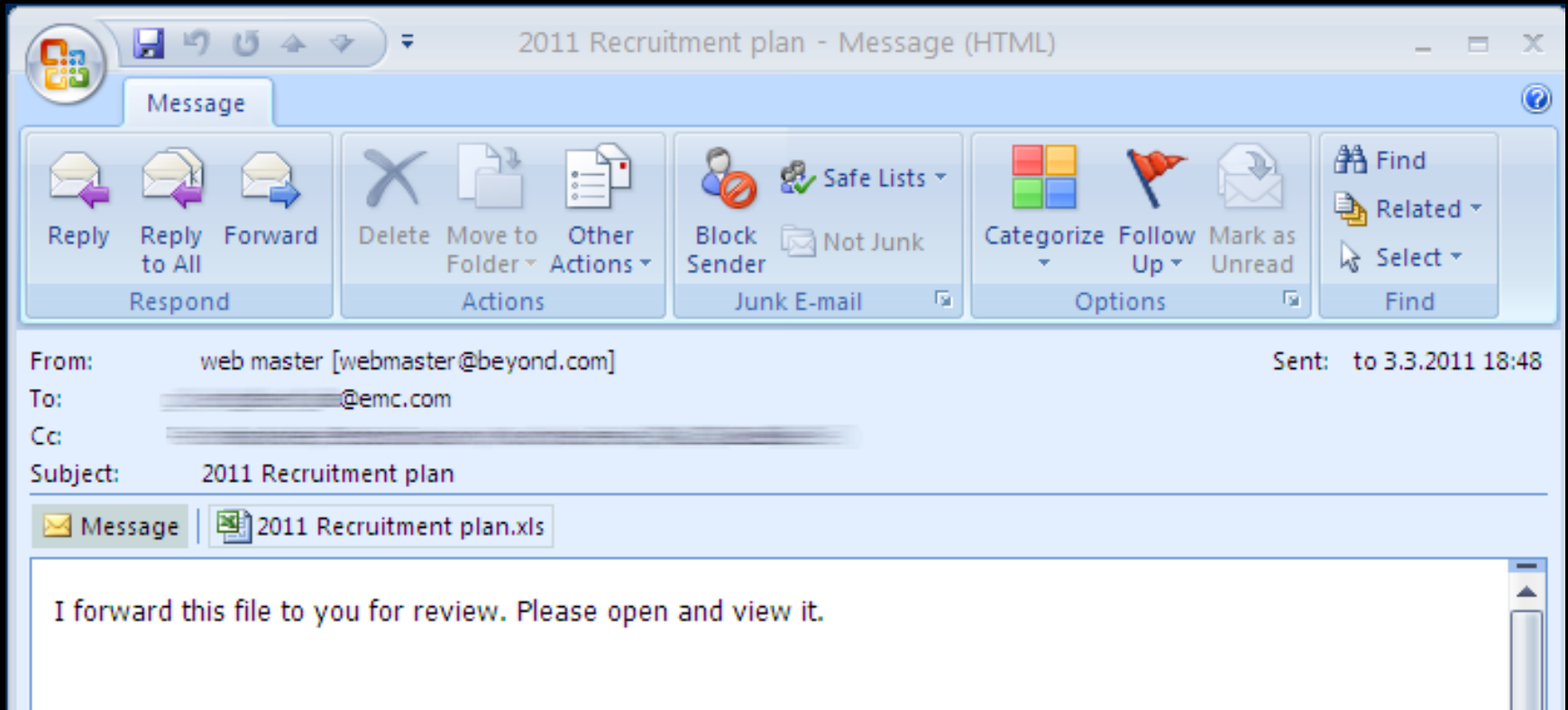
# The Compromised Workstation

- But will my users really fall for social engineering?
  - In short, YES!
  - In many cases, there is no reason for them to suspect
  - Sometimes, no social engineering is required

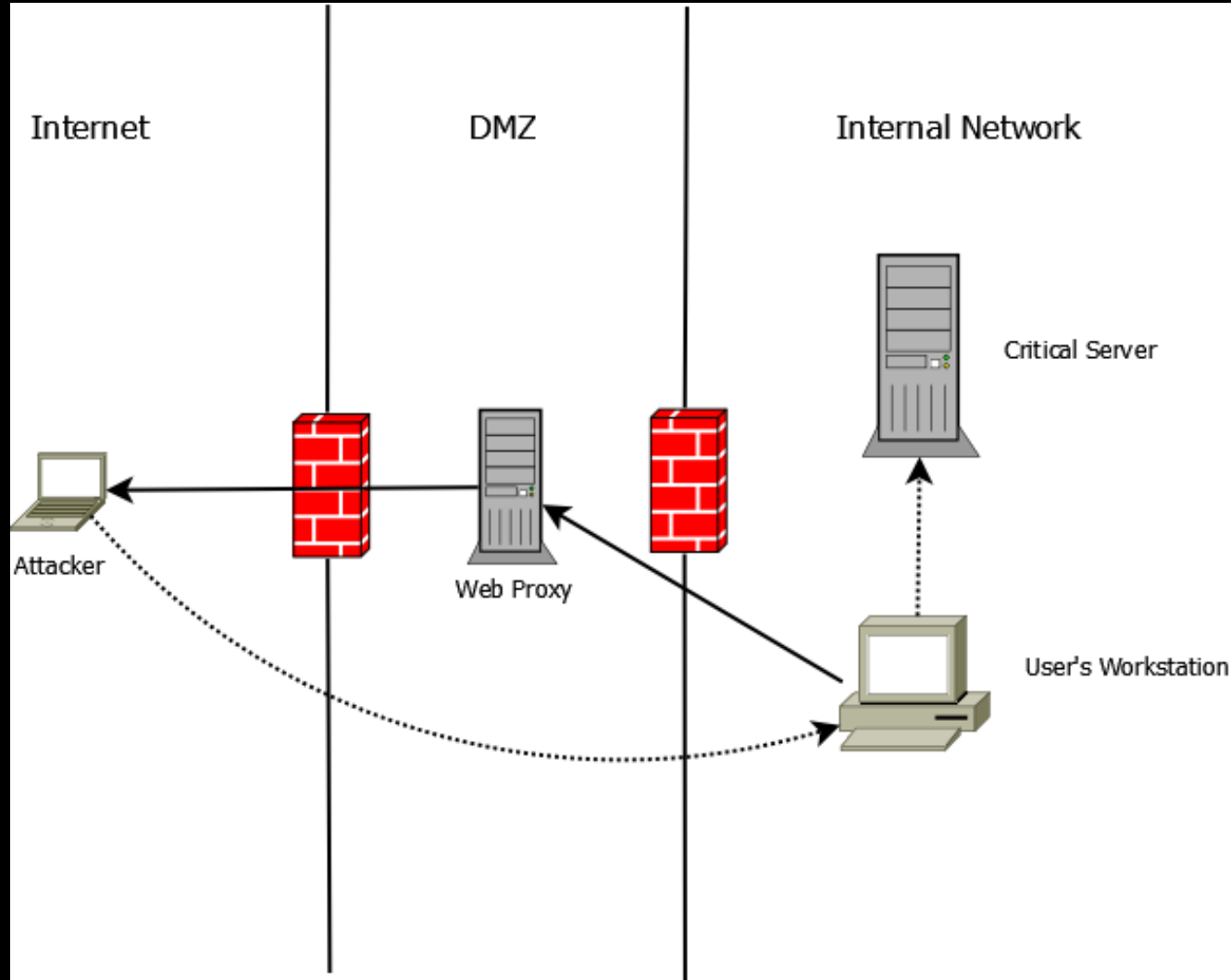


# The Compromised Workstation

- This was the email that compromised RSA (and just about everyone else as a result!)



# Live Demo





## Live Demo

- Internet Explorer Exploit
- Adobe Reader Exploit
- Word Macro Exploit (fully patched machine)
- Local Privilege Escalation
- Post-Exploitation



## Conclusion

- Do not assume your perimeter is secure
- Do not assume your internal network is “trusted”
- You can and will be compromised
- Prepare, Detect and Respond!
- Secure your desktops, harden your internal network



# Questions



