



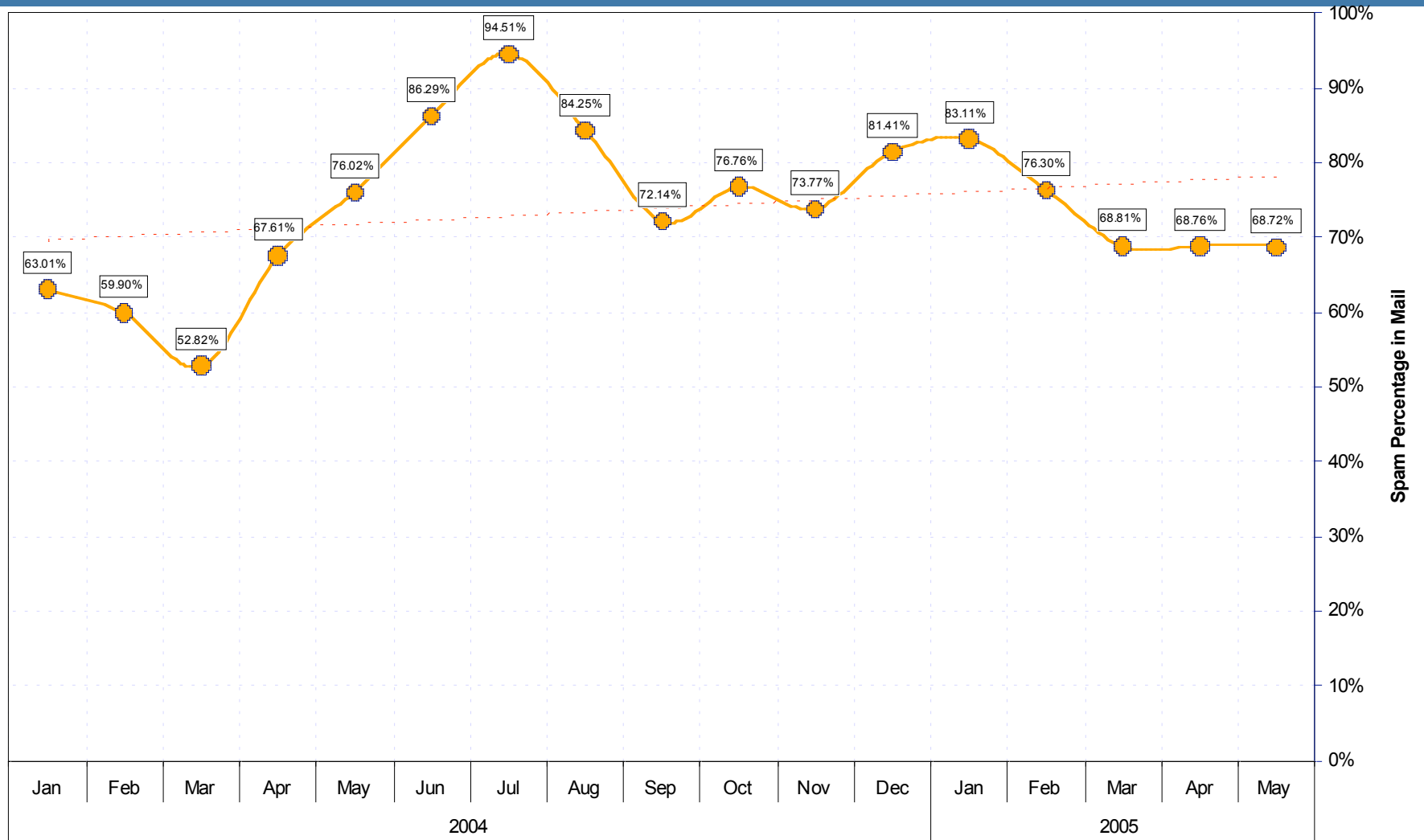
Be certain

Session 12: Technical Standards and Industry Solutions

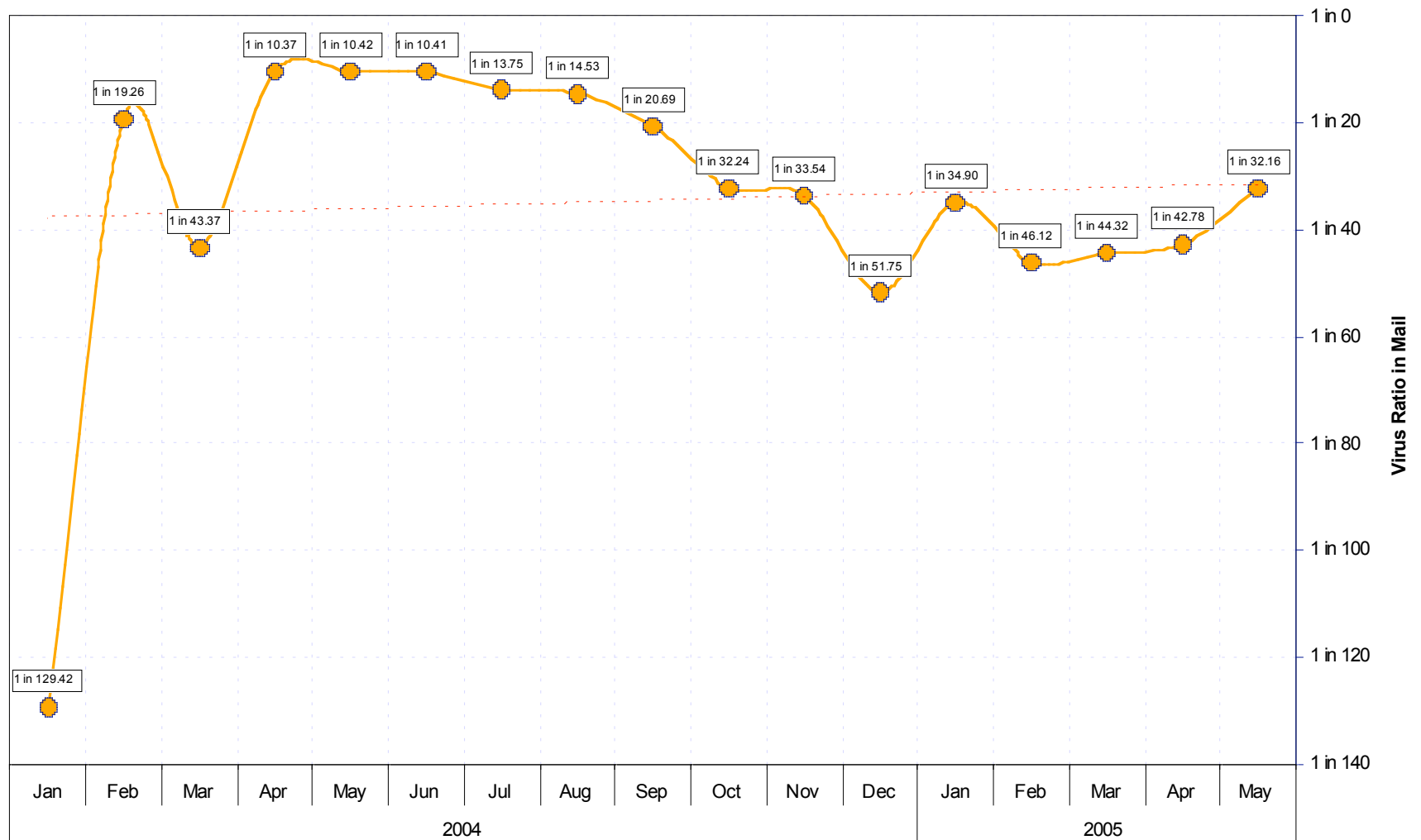
Mark Sunner, Chief Technology Officer

June 30, 2005

Spam Statistics

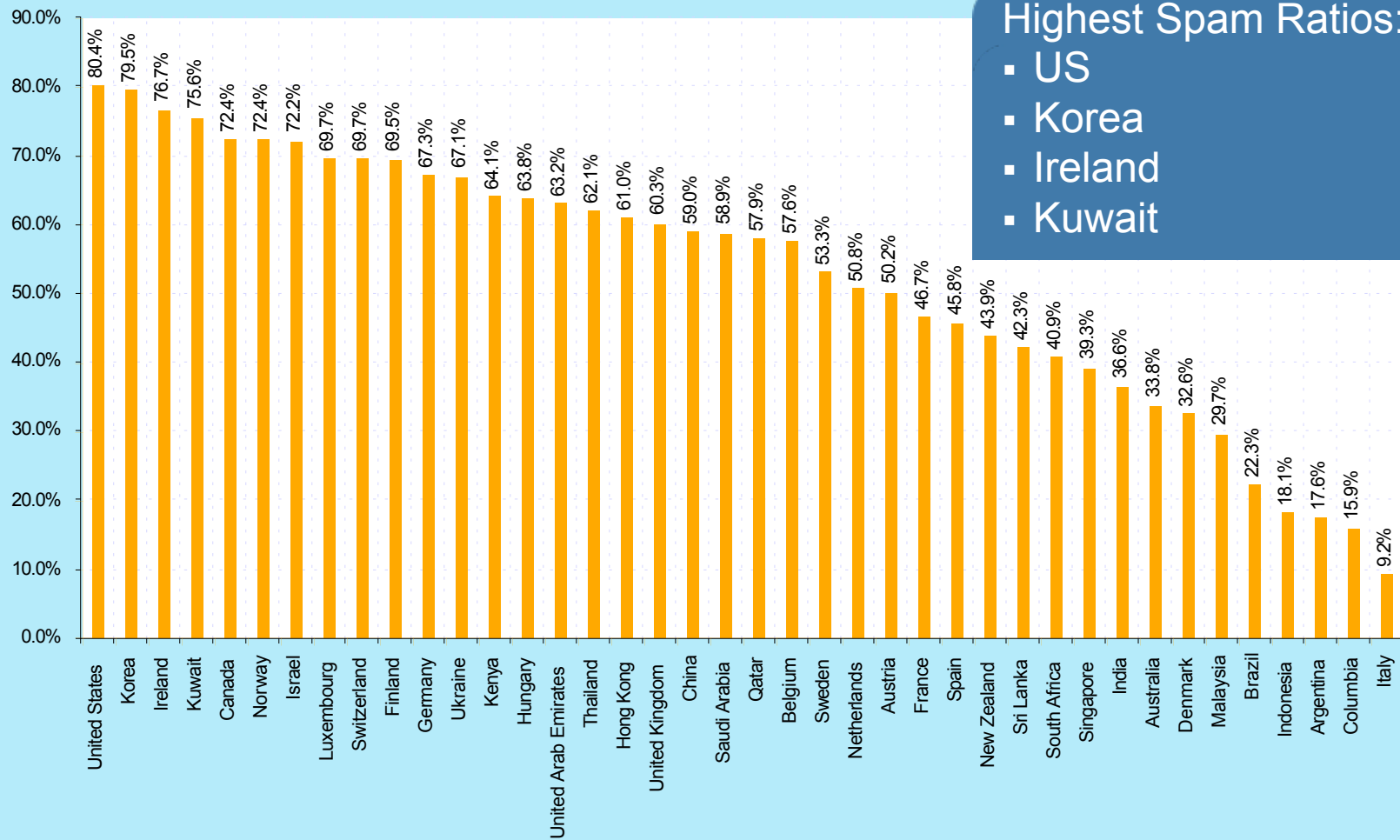


Virus Statistics



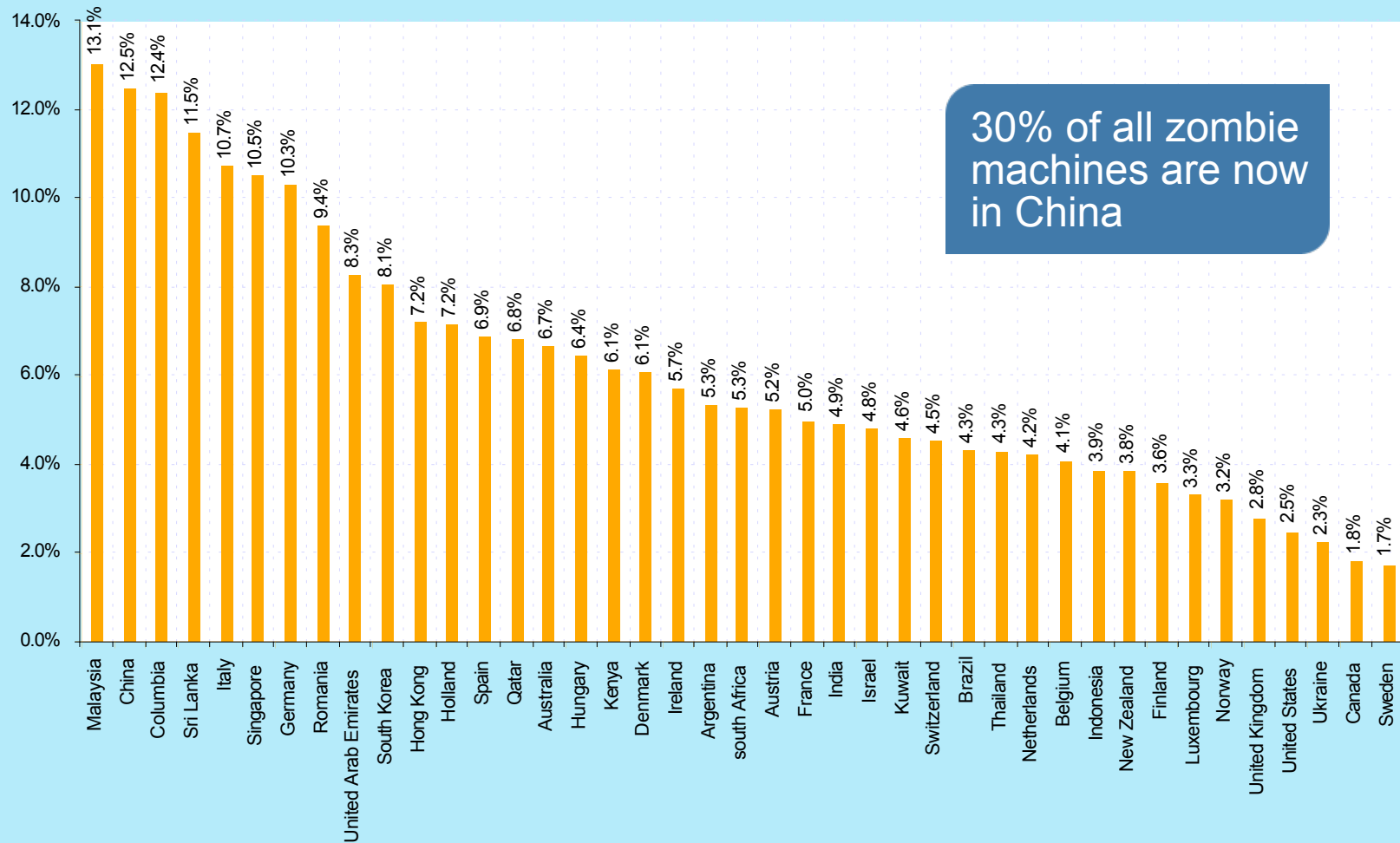
Spam Ratio – May 2005

Geographic Markets

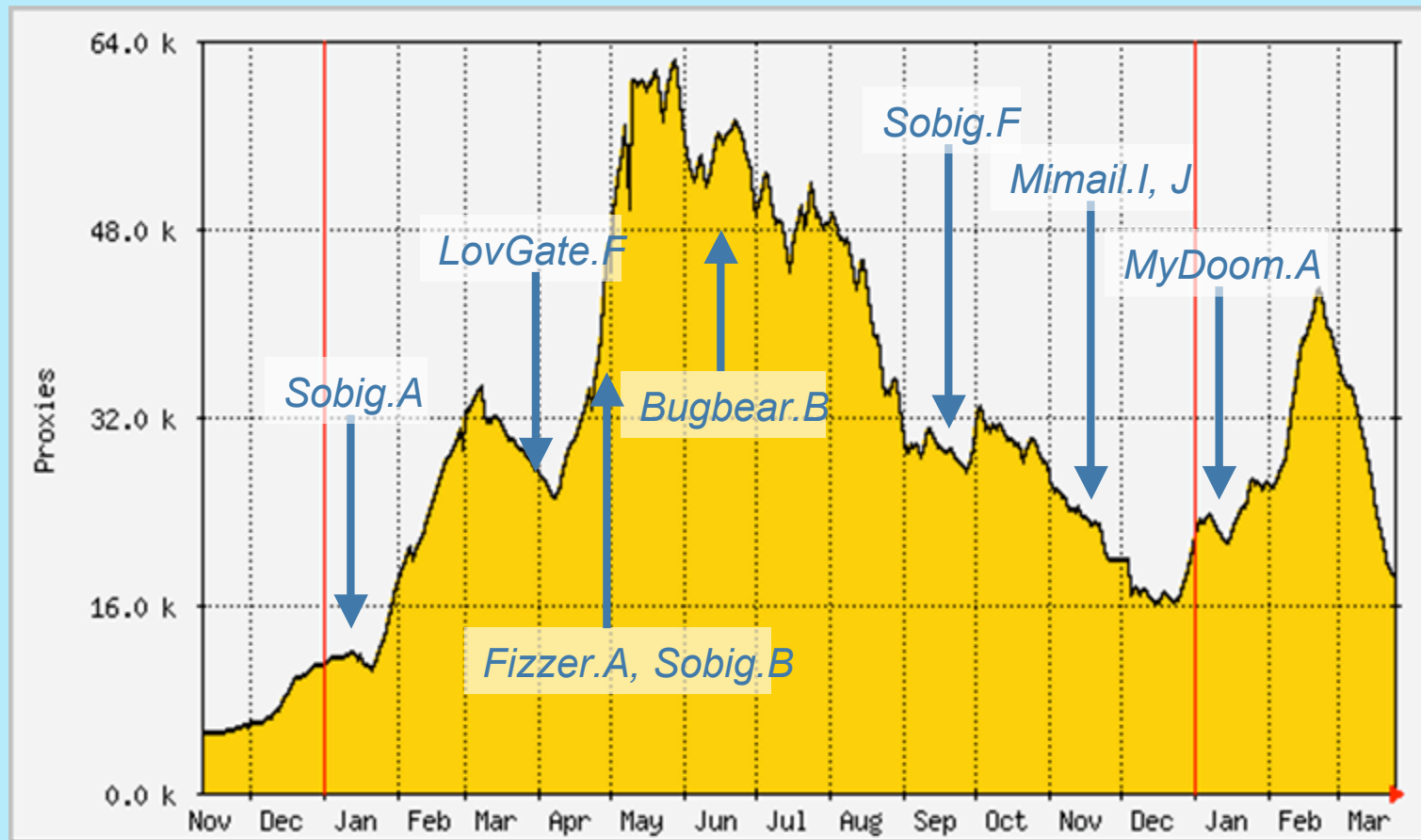


Virus Ratio – May 2005

Geographic Markets



Botnet sign wave



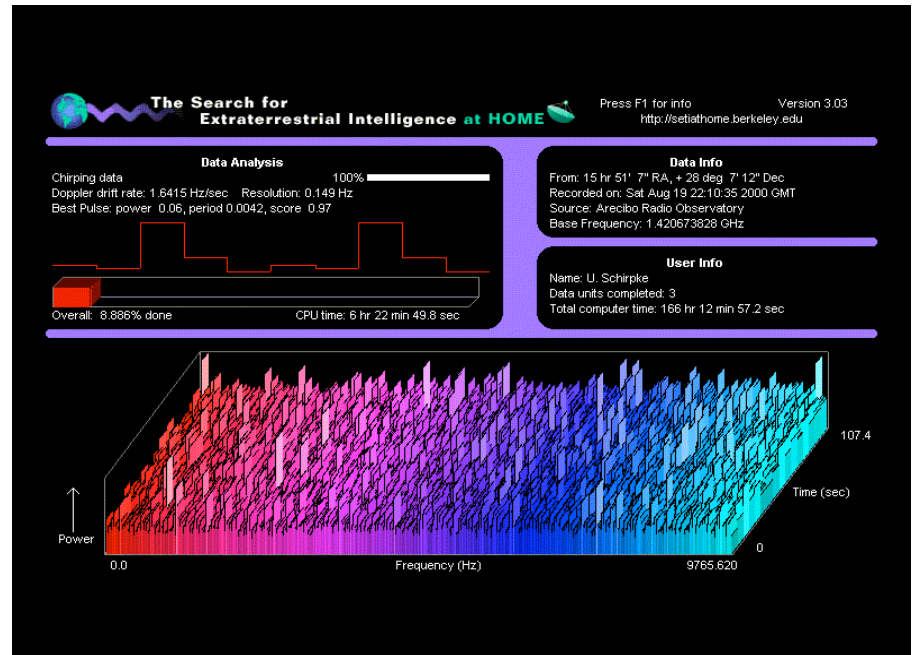
Anatomy of a Botnet



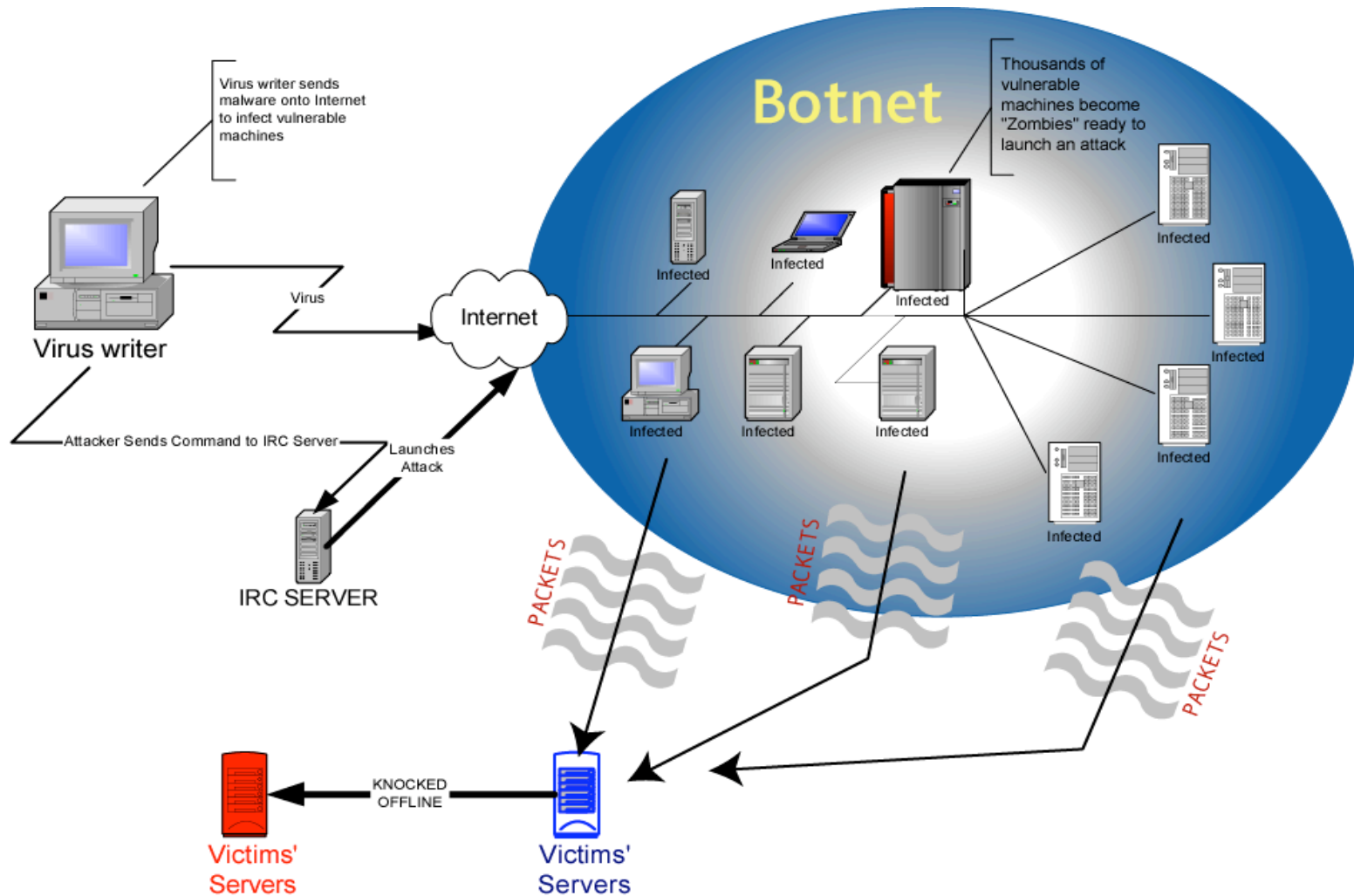
How much Processing Power does a BotNet have?



- The Seti at Home project



Botnets Evolution



SendSafe implications



Send-Safe v2.19b (build 544) - C:\Program Files\Send-Safe

File Run Mail Help

Elapsed: 00:00:00
Sent: 0
Fails: 0

Deliverability: 100%
Avg speed: 30000 mails/hour

- # 1: Ready
- # 2: Ready
- # 3: Ready
- # 4: Ready
- # 5: Ready
- # 6: Ready
- # 7: Ready
- # 8: Ready
- # 9: Ready
- # 10: Ready
- # 11: Ready
- # 12: Ready
- # 13: Ready
- # 14: Ready
- # 15: Ready

Messages | Maillists | Rotation | Settings | Proxies | Advanced | Test

Send test messages

Send email to:

Number of emails to send:

Test the message against SpamAssassin

```
X-Spam-Checker-Version: SpamAssassin 2.70-r6188 (2004-01-17) on HOME
X-Spam-Level: ***
X-Spam-Status: No, hits=2.7 required=5.0 tests=NO_REAL_NAME,ONE_TIM
autolearn=no version=2.70-r6188
```

Test

Resume Start New Pause

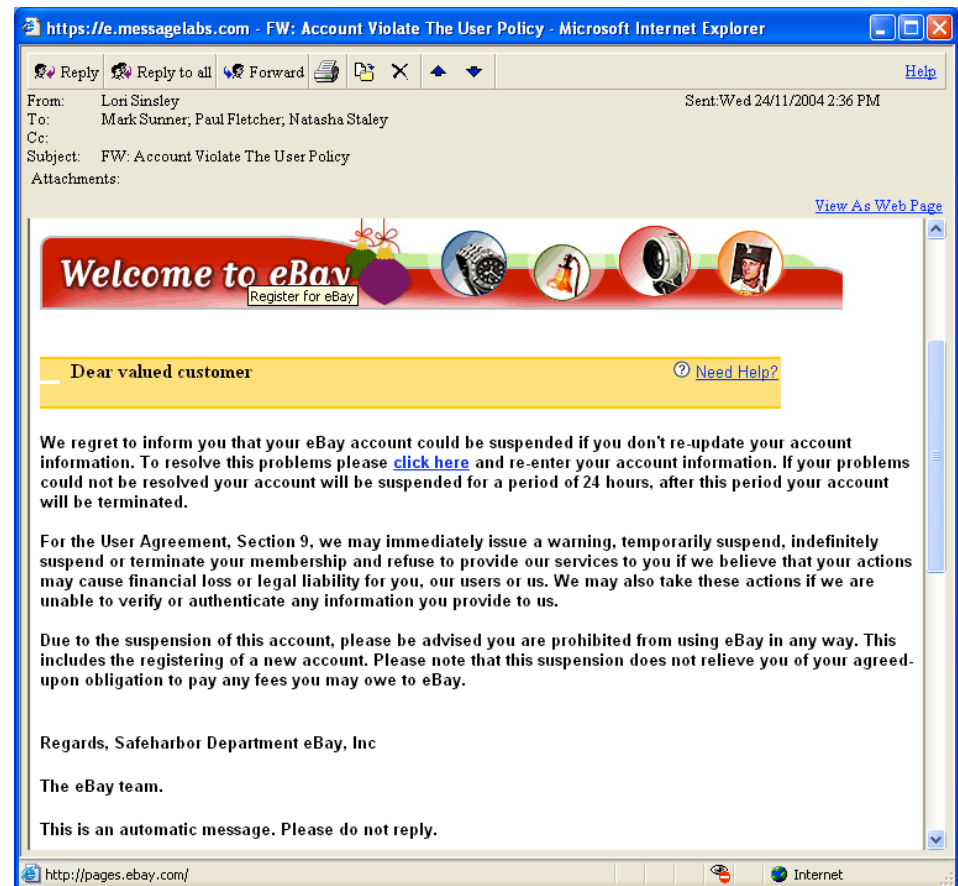
Leased until: 2004-06-24 16:56:56
Credits Total: 10 000 000
Credits Left: 96 075
Message Size: 875 bytes
Processed : 0

23:49:23 Welcome to Send-Safe server!
23:49:23 Latest version is 2.18 beta
23:49:23 http://www.send-safe.com/send-safe.exe

Phishing already SPF compliant



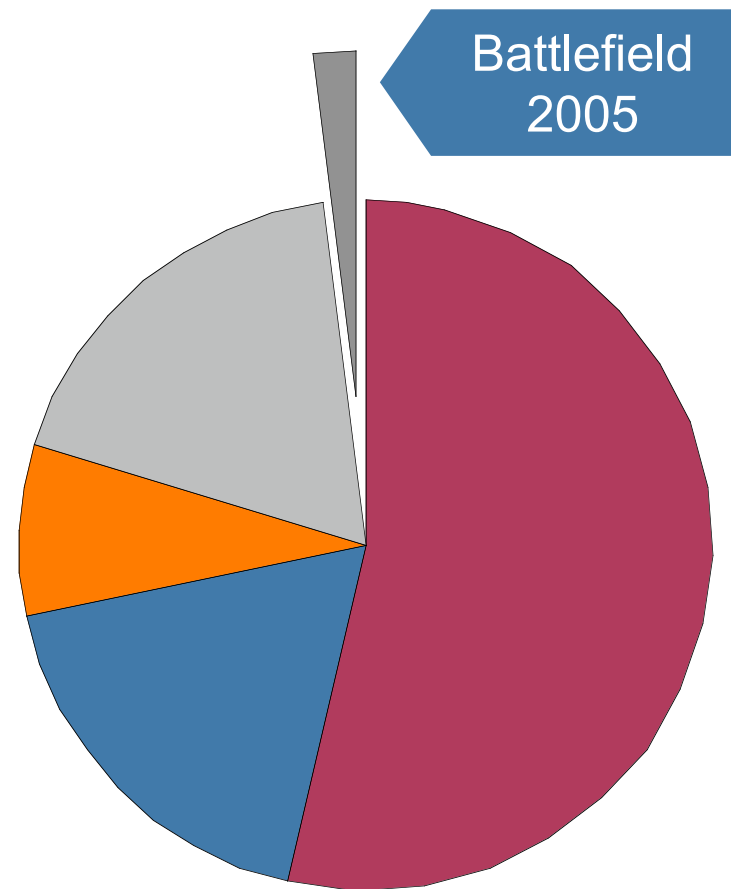
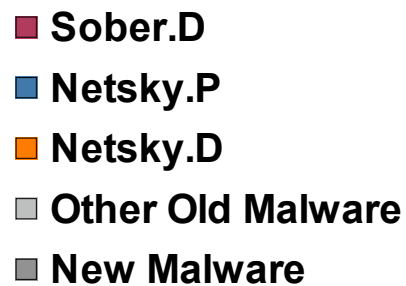
- Valid SPF record published
- Specifies a "soft fail"
 - Accept but subject to normal content checks
- E-bay.com does not belong to ebay.com
 - Validly registered



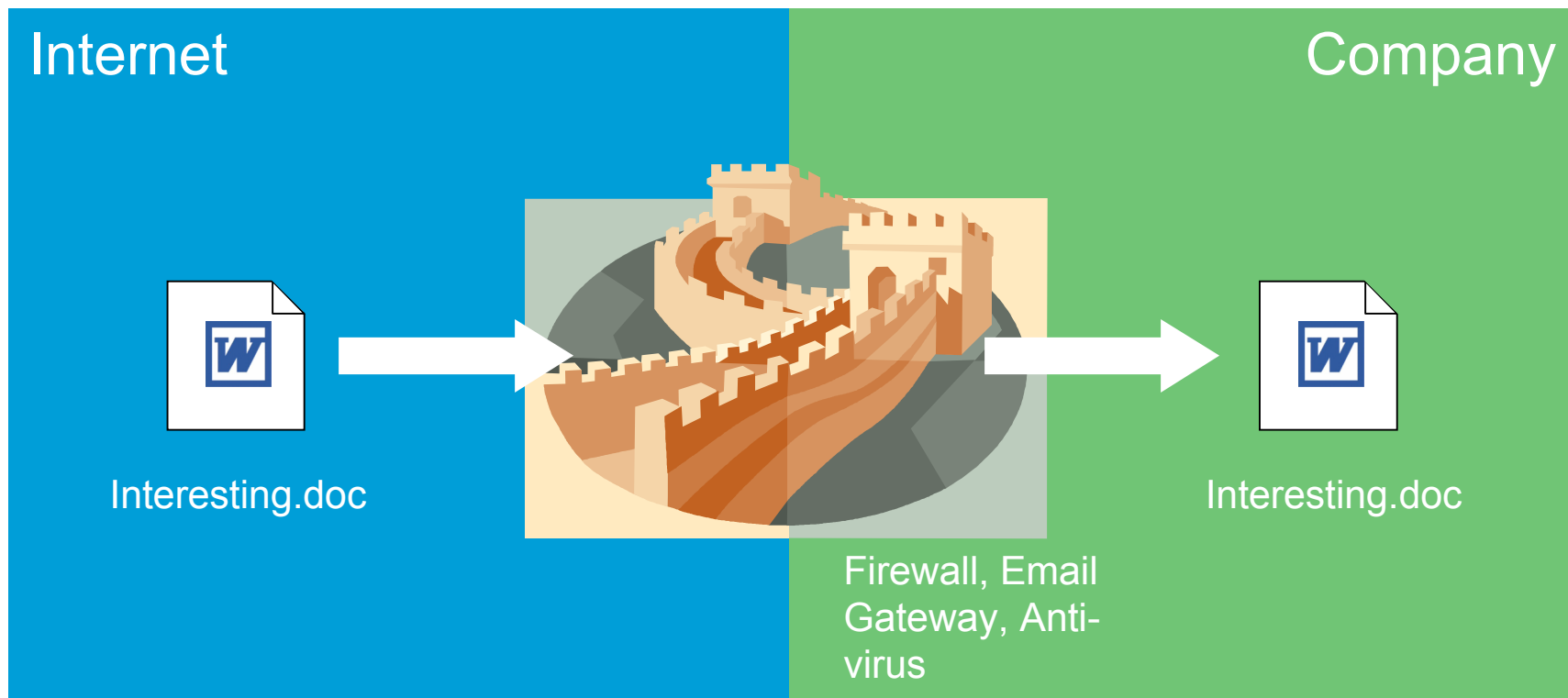
But what should you really be worried about?



- Latest battle – targeted attacks
- ‘Professional’ targeted malware between January and May 2005



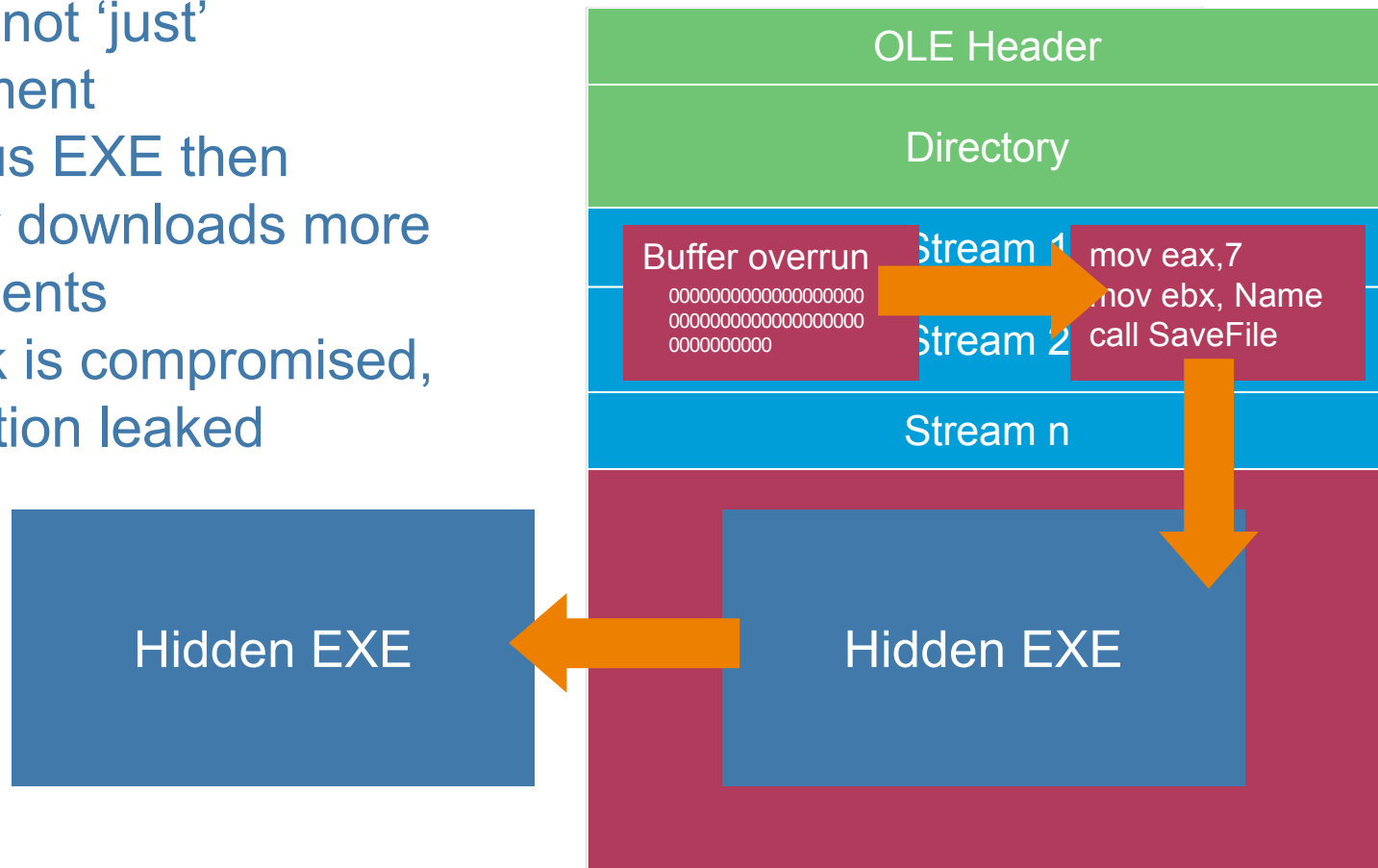
- Typical example



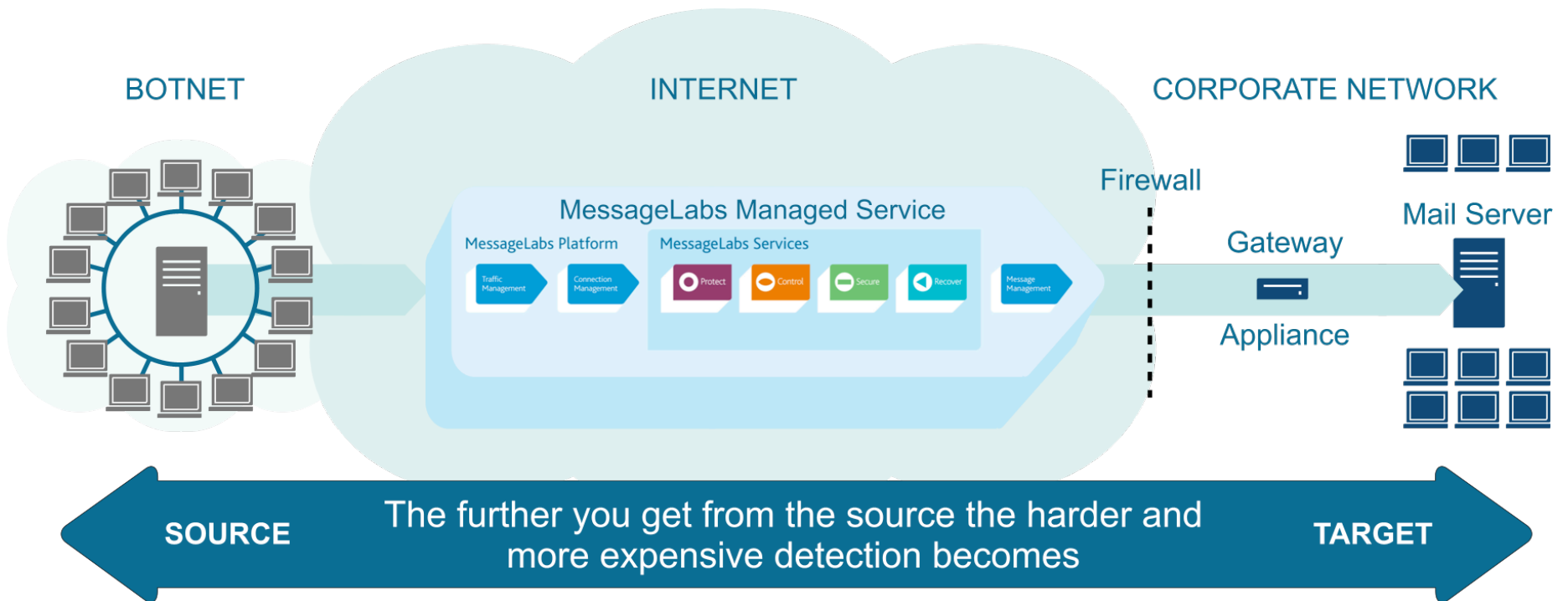
Battlefield 2005



- But it is not 'just' a document
- Malicious EXE then typically downloads more components
- Network is compromised, Information leaked



Move beyond the network and beyond mere scanning



Threat Vision

