



Securing Your Web World



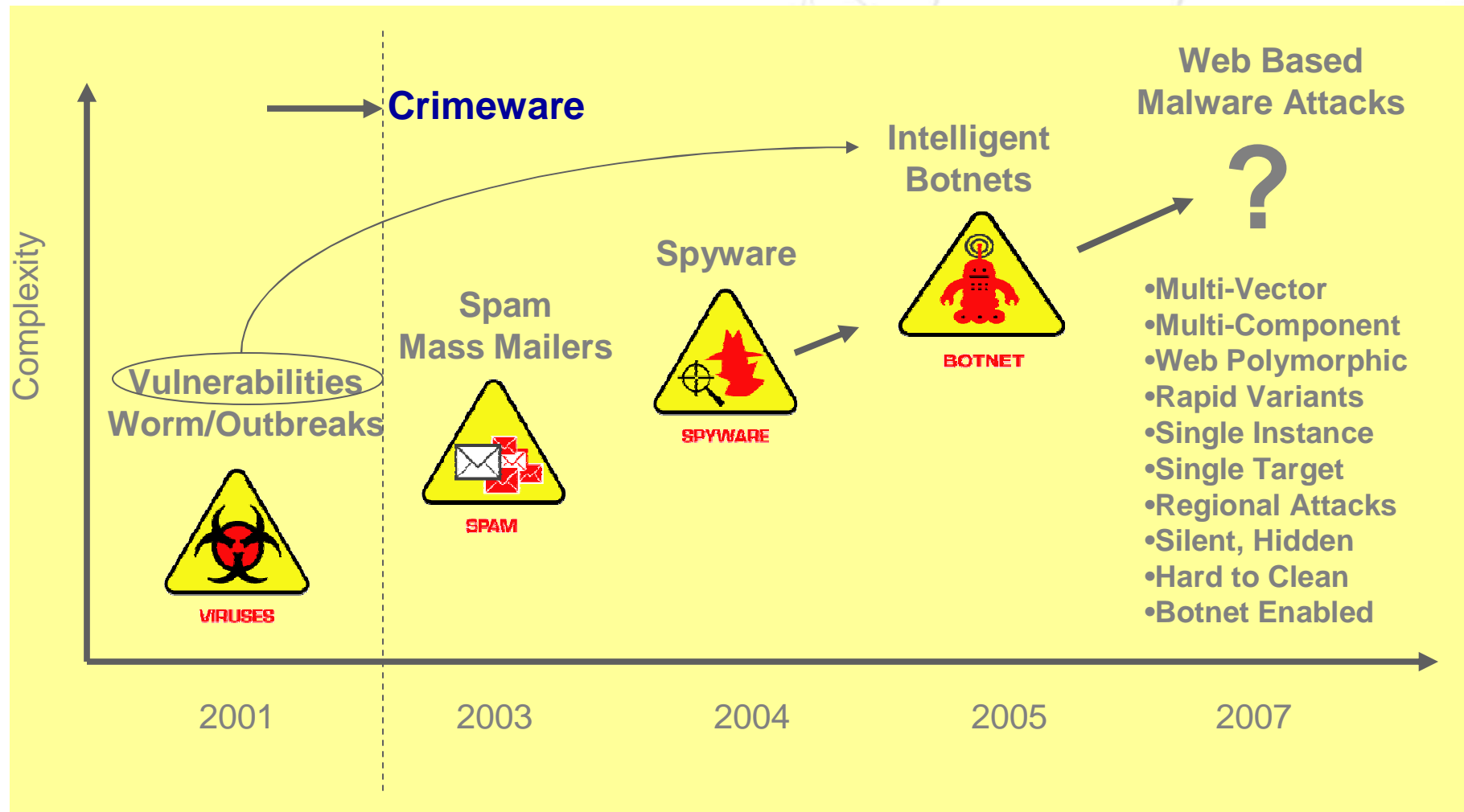
The Evolving Threat Environment –  
**Trend Micro Total Web Threat Protection**

# Stallion Winter Seminar 2008

Veli-Pekka Kusmin  
Pre-Sales Engineer

Trend Micro Channel Confidential  
March 2008

# Threat Environment Evolution to Crimeware



# BOTNETS!

## DEFINITIONS

- Bot:
  - Software robot
  - Allows a system to be controlled remotely without user's knowledge
- Zombie
  - System controlled by a Bot
- Botnet:
  - Network (group) of zombie systems controlled by the Botherder (Botnet owner)



# Money – Money – Money!

## The Security Industry struggles!

Security companies were founded in a time where hackers and malware writers released their creations in the wild to

1. Have fun
2. Show off
3. Highlight Security issues
4. Combat the Evil Commerce aka Microsoft

Now the security industry struggles with organized cybercriminals who

## WANT TO MAKE MONEY



# Malware for Profit is driving Web Threats

Trend Micro  
Securing Your Web World

## Google pulls malicious sponsored links

By Joris Evers

Staff Writer, CNET News.com

Published: April 27, 2007, 5:42 PM PDT

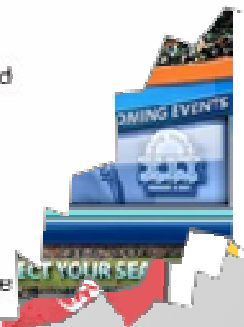
 TalkBack  E-mail  Print  del.icio.us  Digg this



Google has removed paid links that advertised seemingly legitimate Web sites but actually tried to install nefarious programs on PCs.

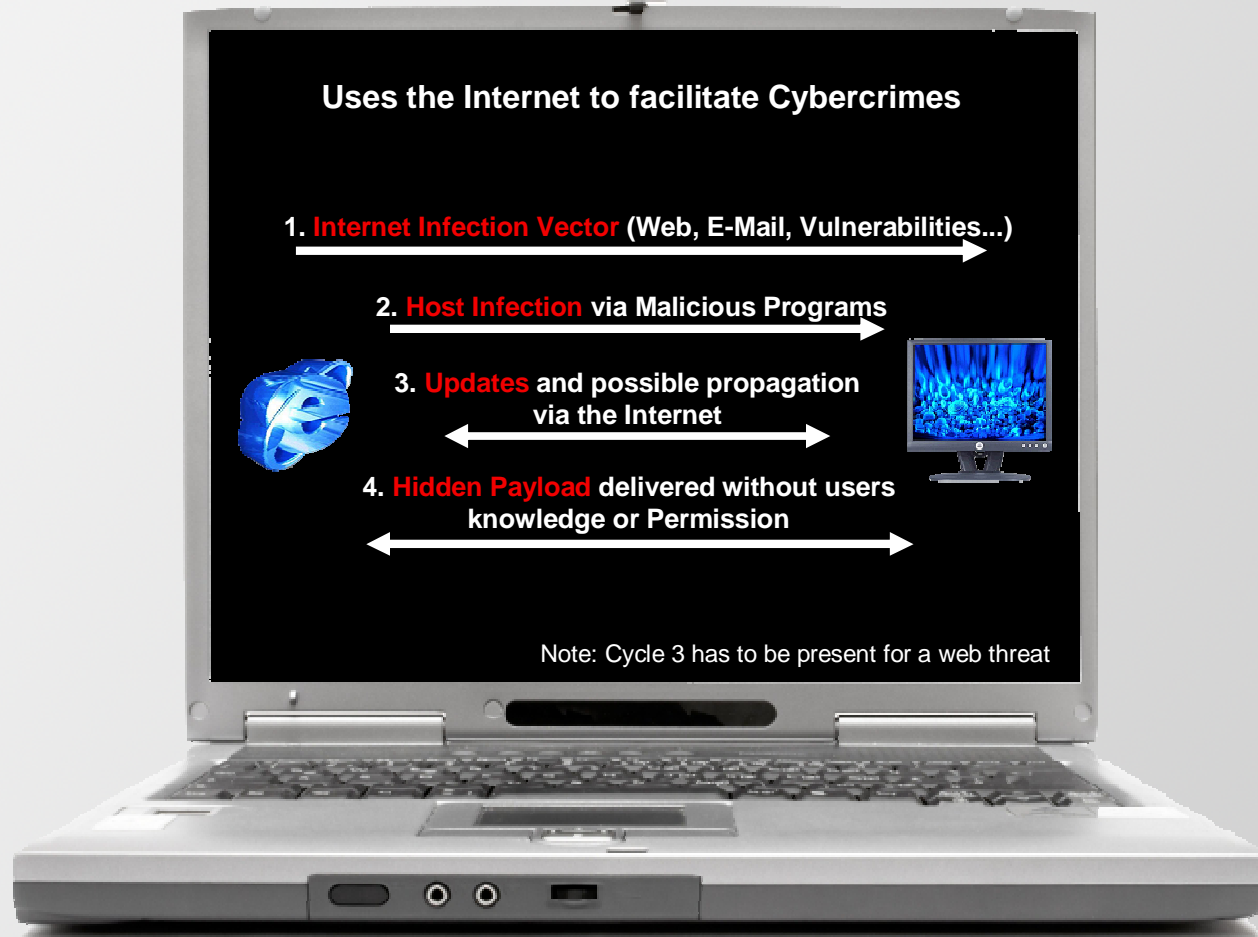
The links were displayed as "sponsored links" after visitors entered specific queries into Google's search service. Clicking the links would ultimately go to a legitimate site, but by way of another site that attempted a "drive-by installation" of password-stealing software. Miscreants placed the links using Google's AdWords service for advertisers.

"Google identified and canceled AdWords accounts displaying ads that re-directed users to malicious sites," a company representative wrote on a corporate blog on Thursday.



Malicious sponsored links

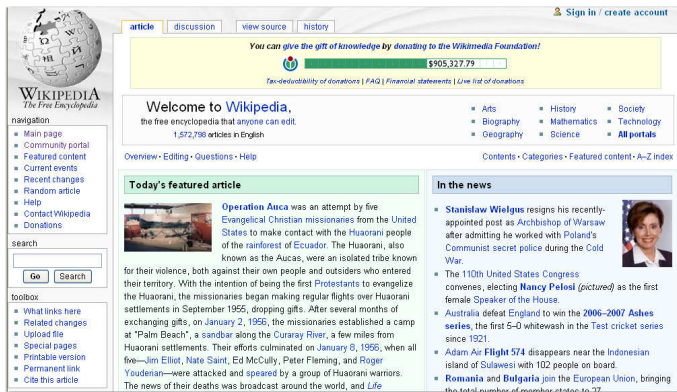
# Web Threats - Revisited



# Key Web Threat Examples

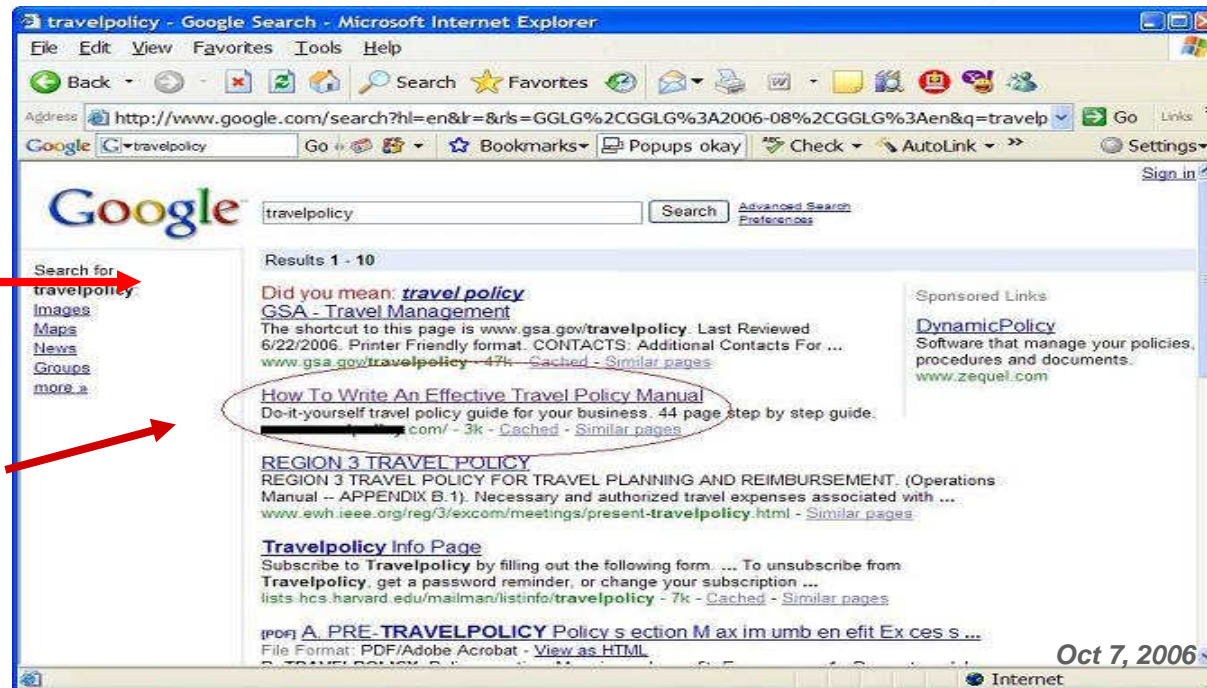
Trend Micro  
Securing Your Web World

- Spyware that was installed upon visiting a website
- Bot that receives commands via IRC or thru web pages
- Adware that was installed after downloading a cool program from the Internet
- Trojan that was installed from a JPEG exploit upon visiting a website that was clicked from an email received
- Virus that was spread from a program downloaded from the internet
- Worm that started blasting copies of itself after disguising itself as a downloadable widget for golfers



# Example: Haxdoor

1. Your boss asks you to develop a corporate travel policy
2. You begin with a Google search on travel policy



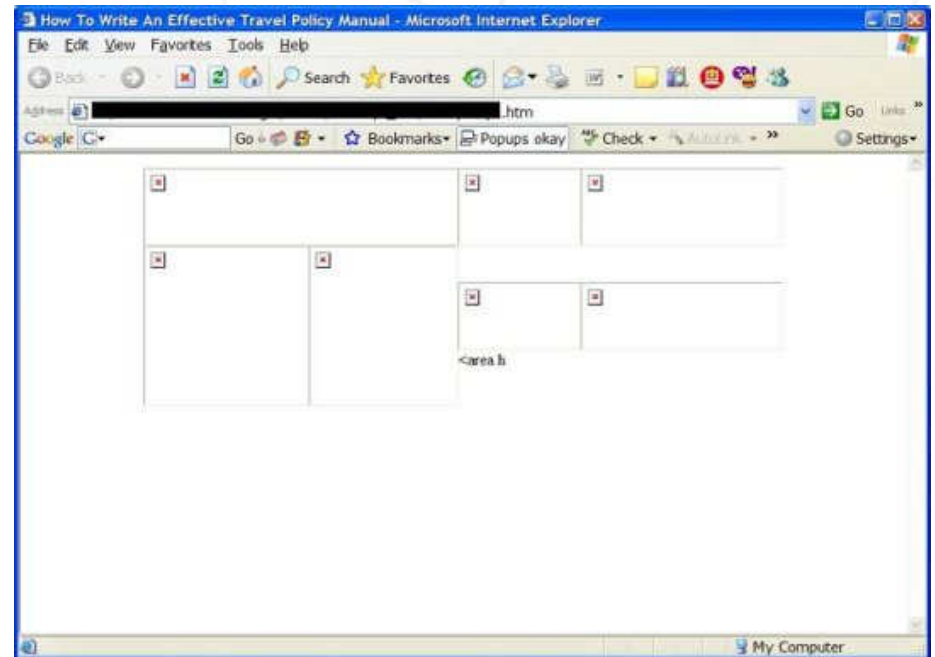
First result is  
a .gov site

Second result  
looks like a  
good choice



# Example: Haxdoor

1. You click on the second search result
2. You wait...the site appears to be downloading images and content...you wait...and you wait...
3. Finally you close the browser window...you'll find another site



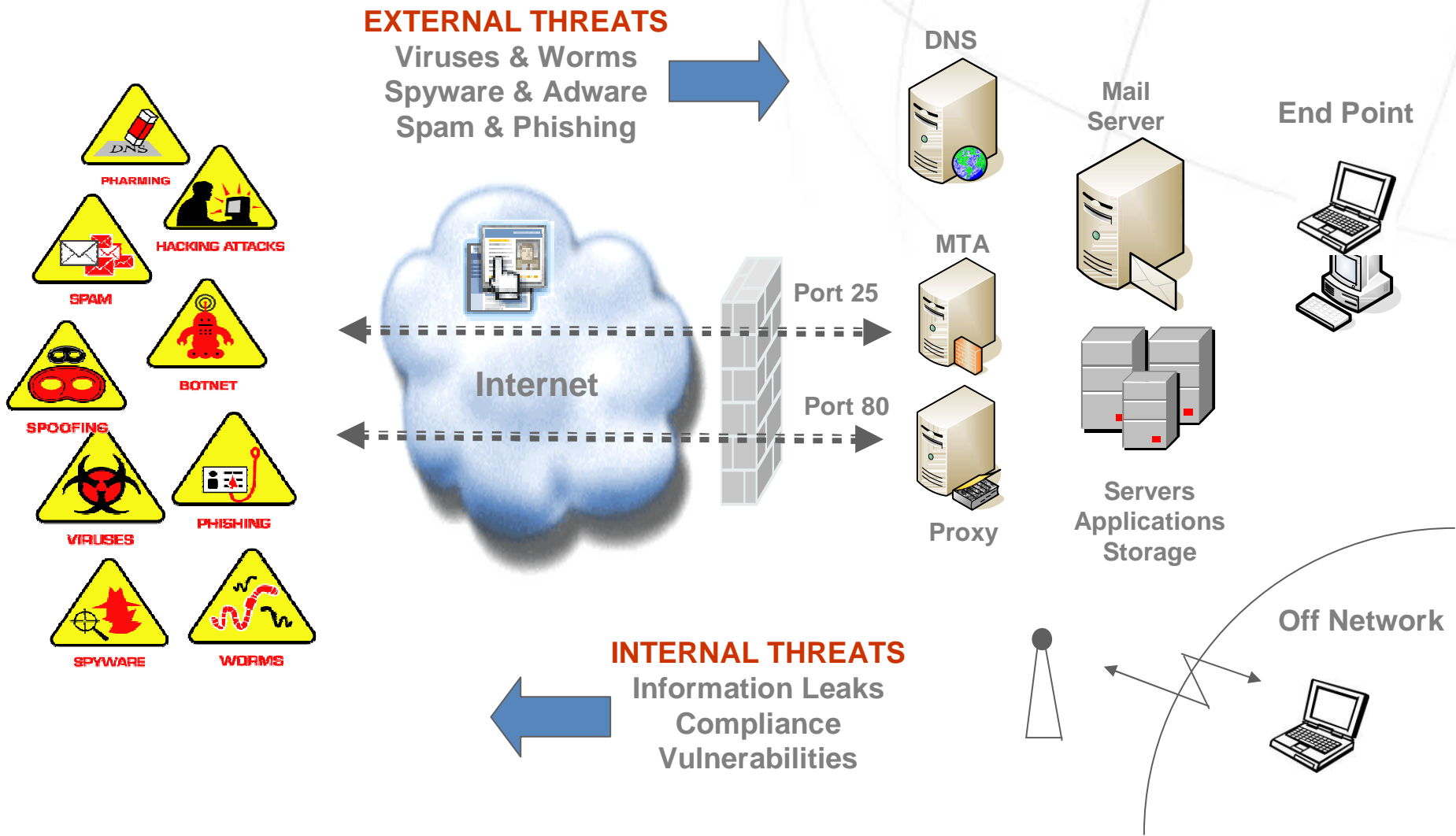
# Example: Haxdoor

## Unbeknownst to you...

1. The IFRAME at the top of the page leads you to an index.html file
2. This file includes a script that exploits the **MS Internet Explorer (MDAC) Remote Code Execution Exploit (MS06-014)**
  - The original exploit code has been modified to try to bypass AV scanners that detect the original exploit
3. An executable file (win.exe) is downloaded to your system and executed
4. You now have a backdoor with rootkit features—a variant of the notorious family of backdoor rootkits known as **Haxdoor!**

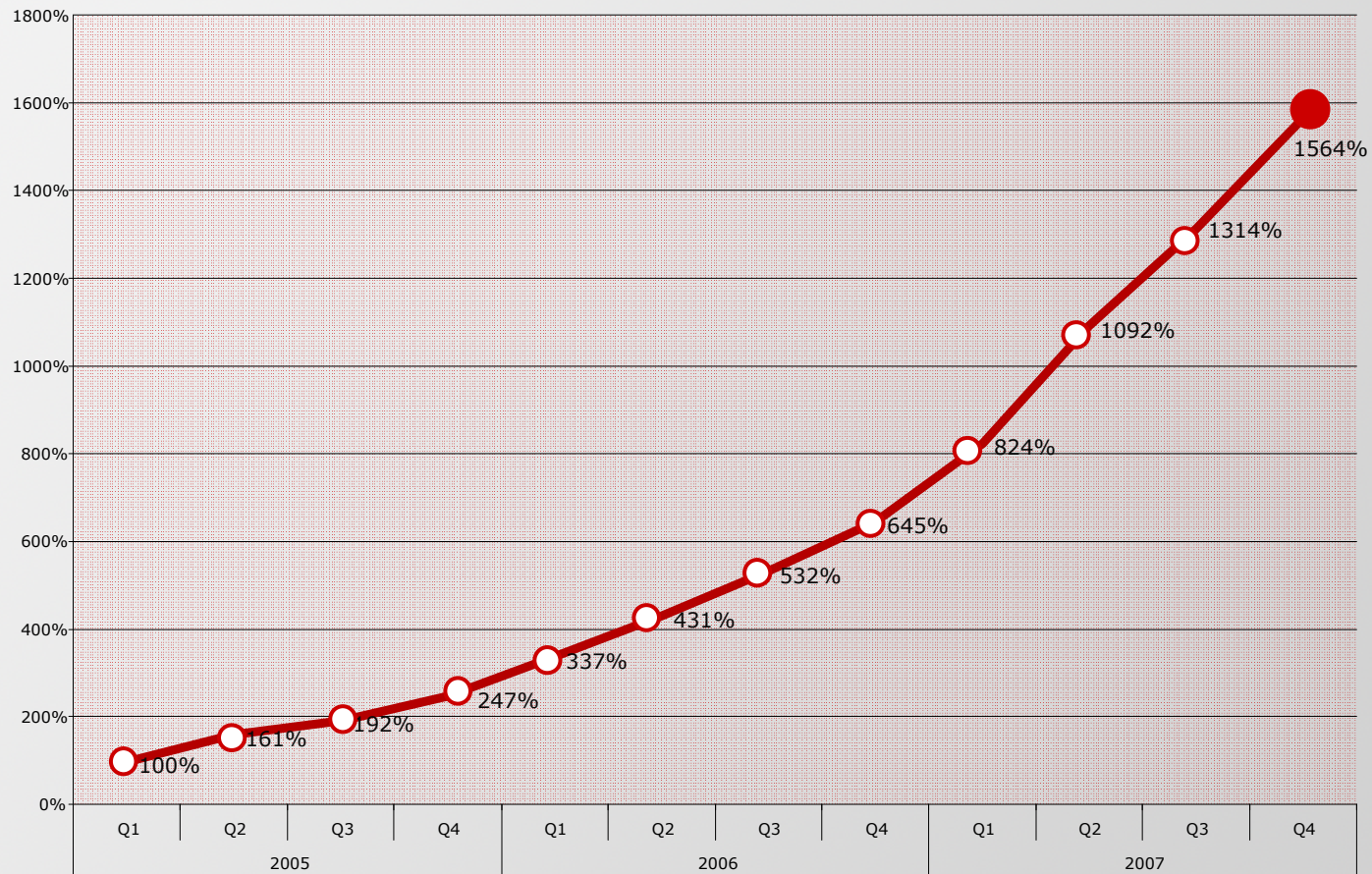
# The Major Threat Vectors are Business Critical

Securing Your Web World



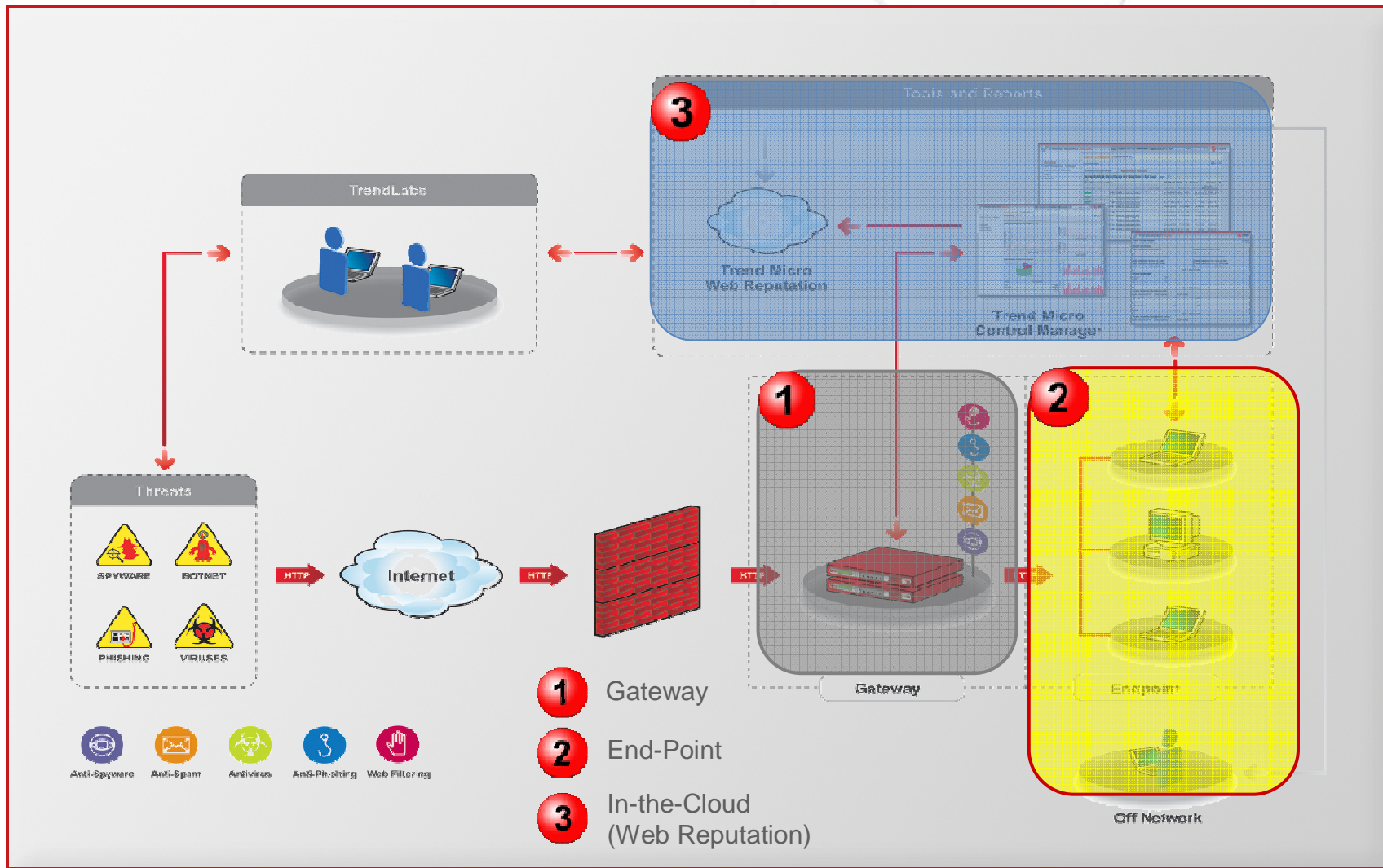
# Threat landscape is shifting to Web-borne attacks

**Web Threats: Total Growth Since 2005**



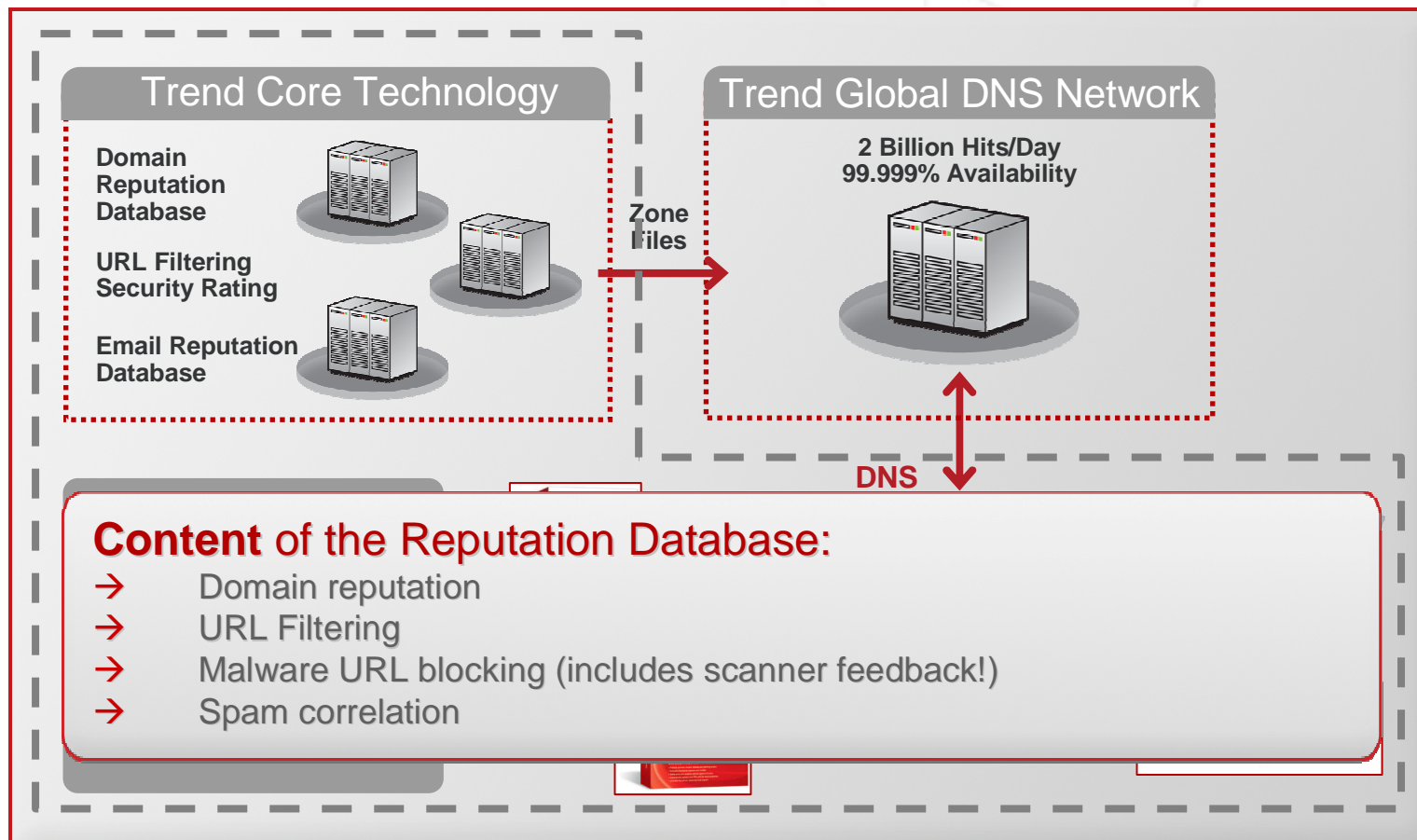
# Total Web Threat Protection: A multi-layered, multi-threat solution

Trend Micro  
Securing Your Web World



# Total Web Threat Protection: Web reputation is unique!

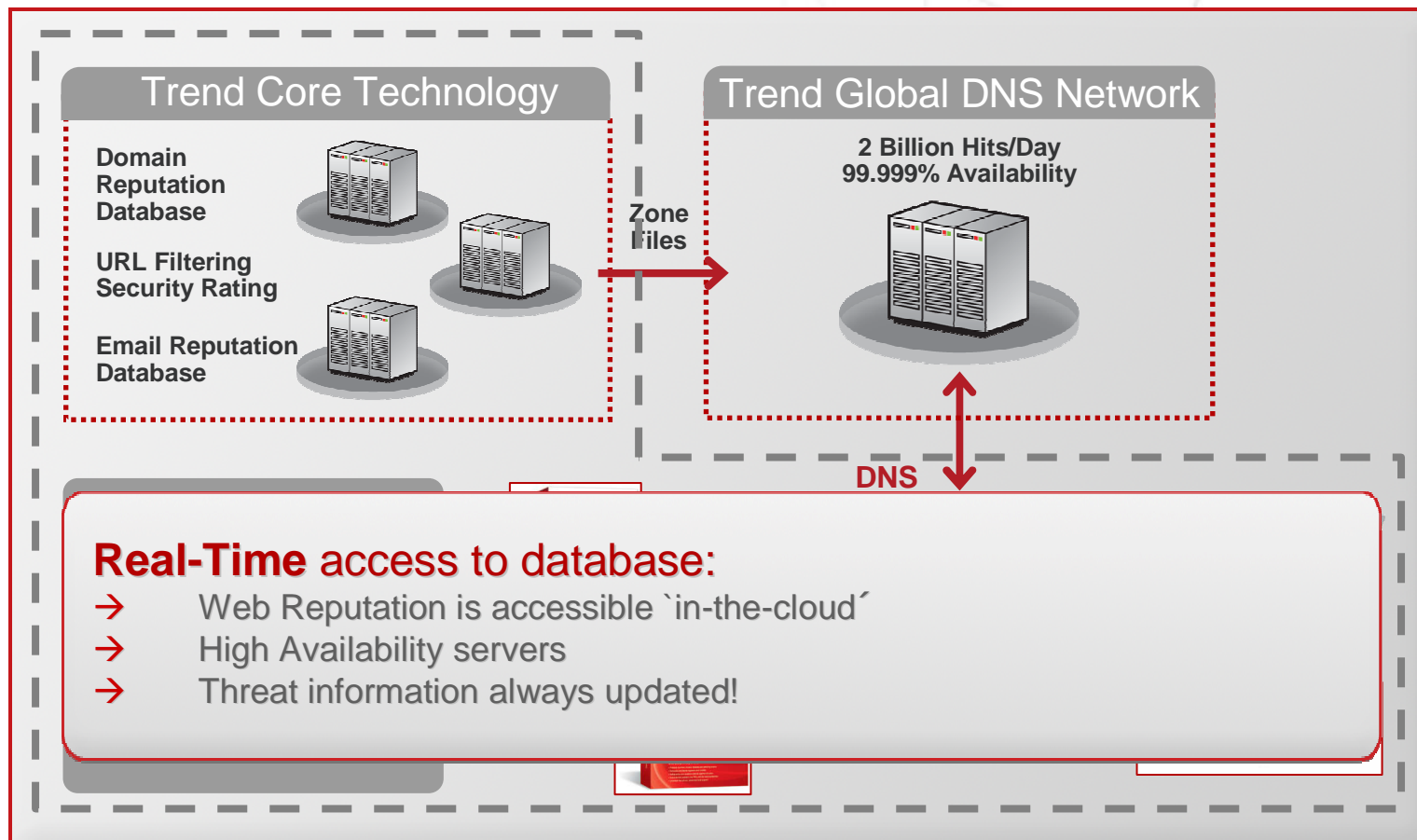
Trend Micro  
Securing Your Web World



The most comprehensive reputation database

# Total Web Threat Protection: Web reputation is unique!

Trend Micro  
Securing Your Web World



No more risks due to missed updates!

# Why Different from URL Filtering Alone?

Trend Micro  
Securing Your Web World

- URL filtering as a Web security solution is like capturing criminals by sending out “WANTED” posters
- Not always up to date
- Only known offenders with previous convictions are listed
- No way to recognize potential new offenders





# Web Reputation is the 21<sup>st</sup> Century Solution

Trend Micro  
Protecting Your Web World

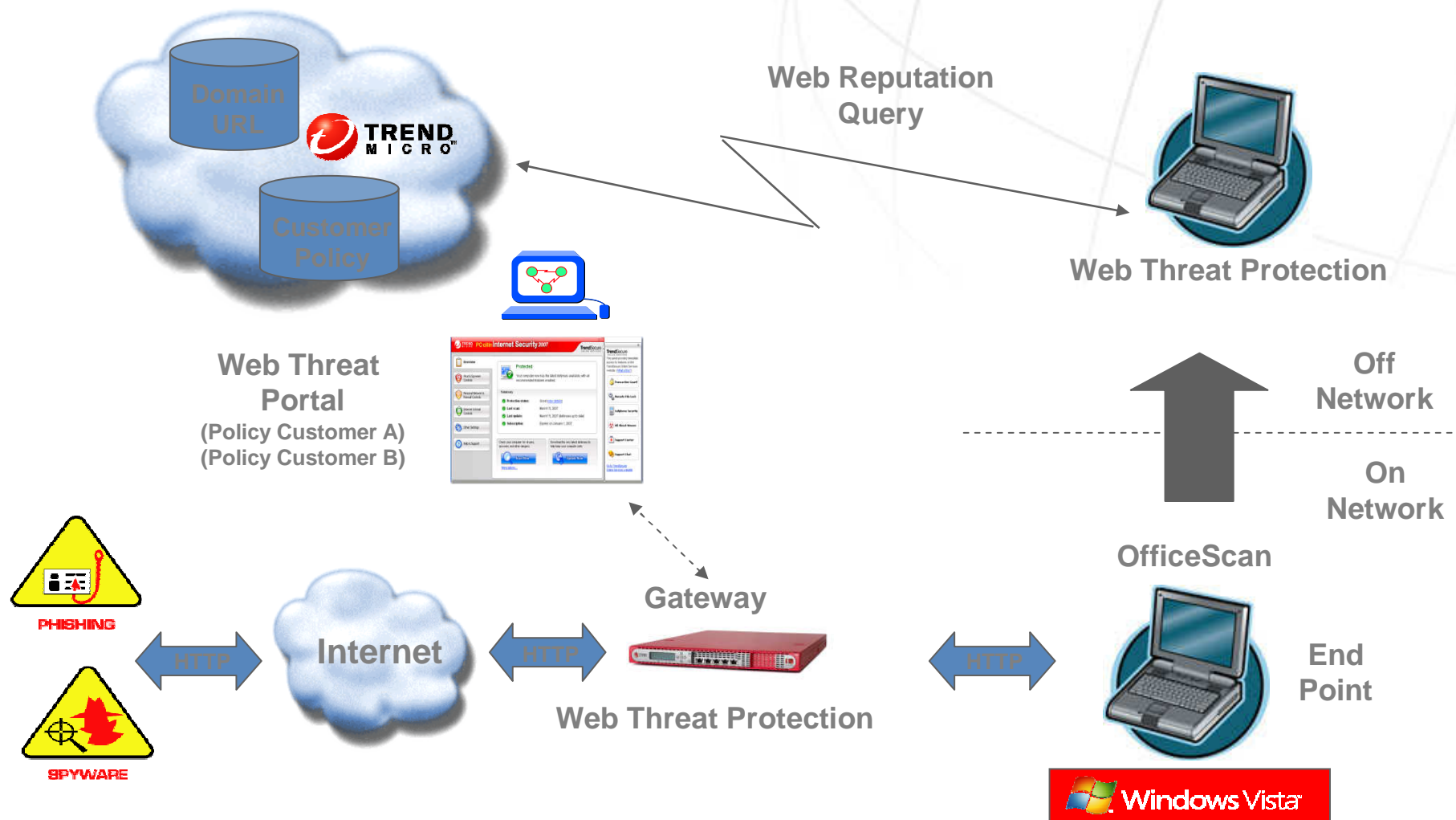
- Exhaustive databases with full profiles on:
  - Known offenders
  - Suspected offenders
  - Possible future offenders
- Constantly updated with input from all over the world
- Instantly accessible by any special agent (Trend product)
- Protect unknown malware and sequential attacks through in-the-cloud Web security rating service
- Web Reputation comprised of 50-plus web site characteristics
  - Static characteristics
  - Historic characteristics
  - Community characteristics
  - Geographic characteristics
  - Web Pages/contents characteristics
  - IP characteristics



# OfficeScan 8: End-point Web Protection

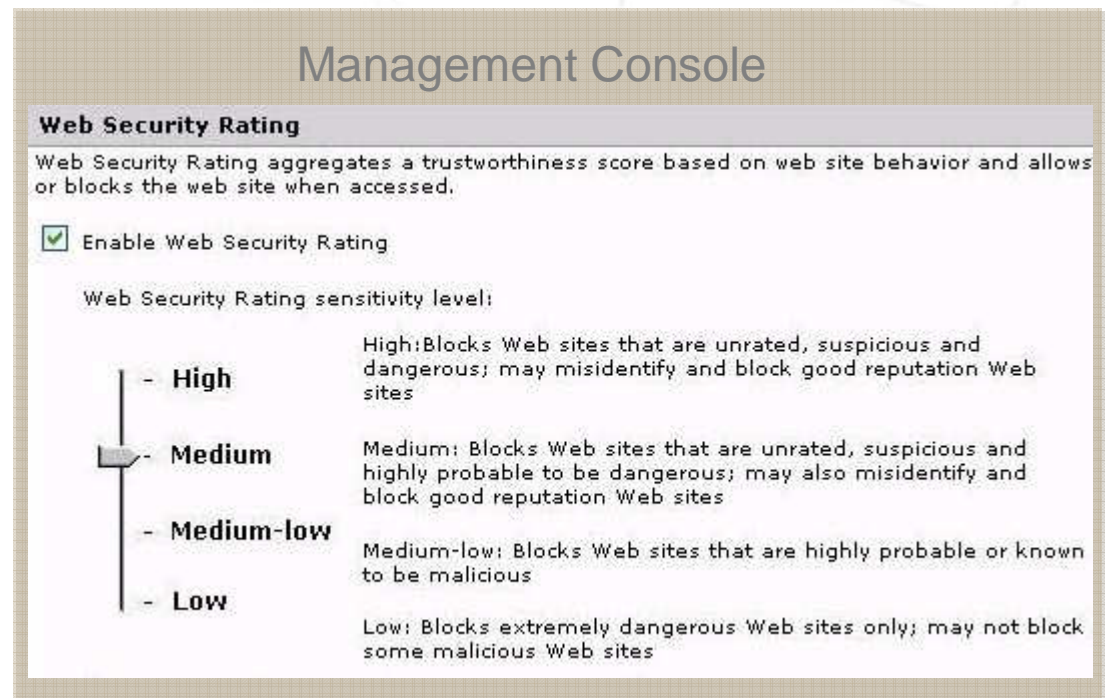
## Mobile Computers On and Off the Network

Trend Micro  
Securing Your Web World



# OfficeScan 8: Adjustable Sensitivity Level Trend Micro Securing Your Web World

- Administrators are allowed to set the protection level based on the query results from Web Reputation
- Actions can be taken upon violation
  - Block, pass but report
- Web Reputation overrides URL filtering policies



The screenshot shows the 'Management Console' interface for 'Web Security Rating'. It includes a title bar, a description of the rating system, a checked checkbox for 'Enable Web Security Rating', and a vertical slider for 'Web Security Rating sensitivity level' with four levels: High, Medium, Medium-low, and Low. Each level has a corresponding description of what sites are blocked.

**Management Console**

**Web Security Rating**

Web Security Rating aggregates a trustworthiness score based on web site behavior and allows or blocks the web site when accessed.

Enable Web Security Rating

Web Security Rating sensitivity level:

- **High** High: Blocks Web sites that are unrated, suspicious and dangerous; may misidentify and block good reputation Web sites
- **Medium** Medium: Blocks Web sites that are unrated, suspicious and highly probable to be dangerous; may also misidentify and block good reputation Web sites
- **Medium-low** Medium-low: Blocks Web sites that are highly probable or known to be malicious
- **Low** Low: Blocks extremely dangerous Web sites only; may not block some malicious Web sites

# OfficeScan 8: What the IT Admin Sees

Trend Micro  
Securing Your Web World

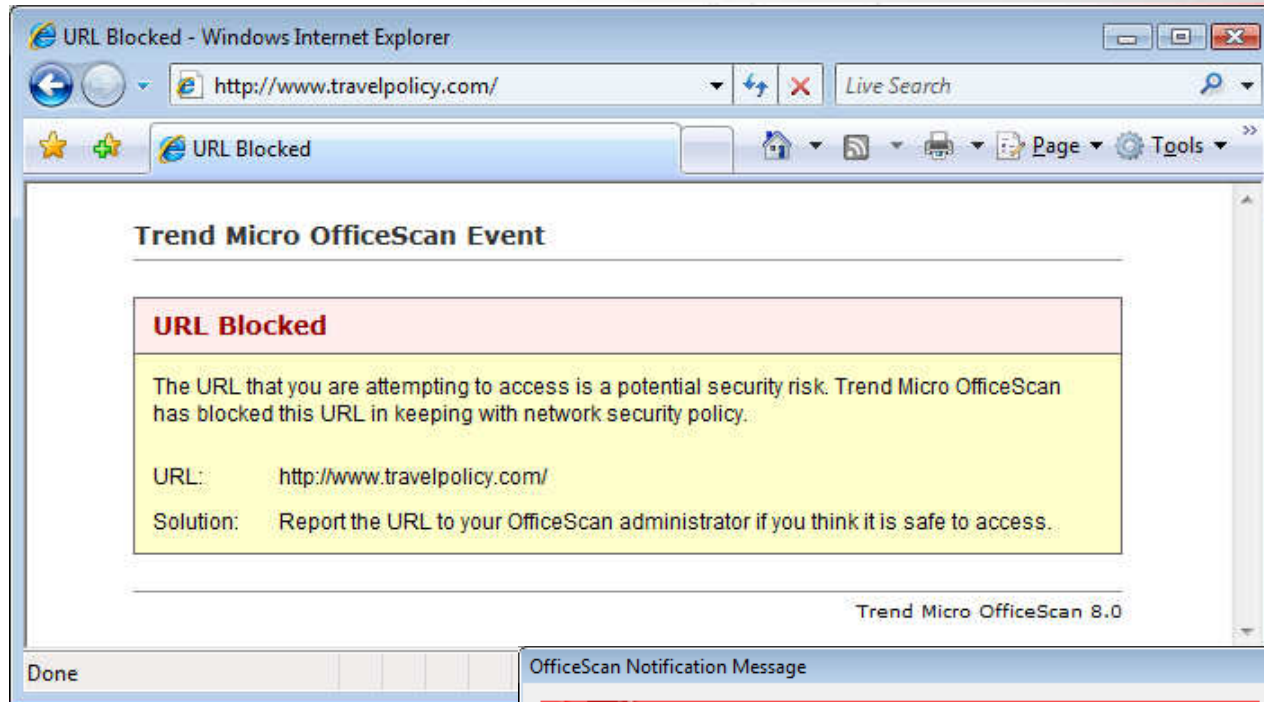
The screenshot shows the 'Web Reputation Policies' configuration page in the OfficeScan 8 web interface. The page is divided into several sections:

- External Computers / Internal Computers:** The 'Internal Computers' tab is selected.
- Enable Web Reputation policy:** A checked checkbox.
- Security Level:** Radio buttons for 'High', 'Medium', 'Medium-low', and 'Low'. 'Medium' is selected.
- Approved URL List:** A table listing approved URLs and their coverage. A text input field contains 'http://', and an 'Add >>' button is next to it.
- Client Log:** A checkbox for 'Allow clients to send logs to the OfficeScan server' is unchecked.

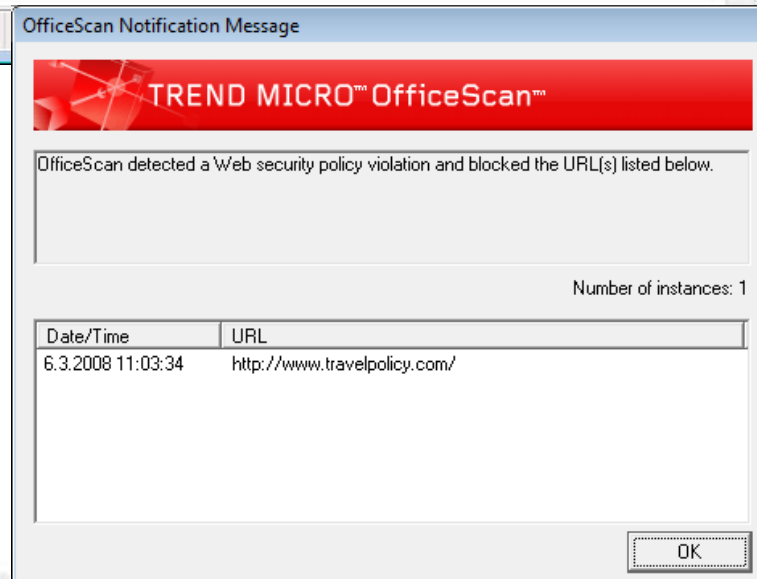
Approved URL	Coverage
http://www.trendmicro.com	All subsites
http://kb.trendmicro.com	All subsites
http://windowsupdate.microsoft.com	All subsites
http://wustat.windows.com/wustrack.bin?*	This page only
http://download.windowsupdate.com	All subsites
http://office.microsoft.com	All subsites
http://c.microsoft.com	All subsites
http://download.microsoft.com	All subsites
http://servicecenter.antivirus.com	All subsites
http://uk.trendmicro-europe.com	All subsites
http://housecall.antivirus.com	All subsites

# OfficeScan 8: What the End-user Sees

Browser:



Client popup:



# Real-time stats on web reputation


Trend Micro  
Securing Your Web World

## Internet Pollution Ticker

Tracking the prevalence of threats on the Web  
Based on Trend Micro's Web threat protection technology


## http://www.am-i-ok.com

**Web Threats**




Web threats are any threat that uses the Web to do bad and unwanted things. Web Threats are increasing dramatically—540% increase since 2005.

**Web Activity Monitored**



Every day, Trend Micro checks over 3 billion URLs for malicious code

**Malicious Activity Prevented**



And, through its Web threat protection technology, Trend Micro breaks 8-10 million infections daily

Last Month ▾

Last Month ▾


<p><b>Malicious Websites</b></p> <p style="text-align: center;">22.6%</p> <div style="width: 20%; height: 10px; background: linear-gradient(to right, yellow, orange);"></div> <p style="text-align: center; font-size: small;">of URL Requests</p>	<p>URL requests scanned</p> <p style="text-align: center; font-size: large;">10105090611</p>	<p>Malicious URLs <b>blocked</b></p> <p style="text-align: center; font-size: large;">2283488008</p>	<p><b>Malicious Websites</b></p> <p style="font-size: x-small;">Trend Micro Web threat protection allows user's to view the page content <b>blocking malicious content</b></p> <p style="text-align: right; color: red; font-size: x-small;"><a href="#">Learn More &gt;&gt;</a></p>
<p><b>Spam</b></p> <p style="text-align: center;">91.2%</p> <div style="width: 20%; height: 10px; background: linear-gradient(to right, yellow, orange);"></div> <p style="text-align: center; font-size: small;">of Email Requests</p>	<p>E-Mail scanned</p> <p style="text-align: center; font-size: large;">7625012658186</p>	<p>Spam <b>blocked</b></p> <p style="text-align: center; font-size: large;">6954034641616</p>	<p><b>Spam</b></p> <p style="font-size: x-small;">Trend Micro e-mail reputation scanning <b>blocks e-mail</b> with malicious links or attachments and attacks such as phishing and pharming</p> <p style="text-align: right; color: red; font-size: x-small;"><a href="#">Learn More &gt;&gt;</a></p>
<p><b>Malware</b></p> <p style="text-align: center;">6.2%*</p> <div style="width: 10%; height: 10px; background: linear-gradient(to right, yellow, orange);"></div> <p style="text-align: center; font-size: small;">of File Transfers</p>	<p>File scanned</p> <p style="text-align: center; font-size: large;">8872112074526</p>	<p>Malware Files <b>blocked</b></p> <p style="text-align: center; font-size: large;">550070929833</p>	<p><b>Malware</b></p> <p style="font-size: x-small;">Trend Micro <b>multi-tiered protection</b> scans files for malware in the cloud, at the gateway, and on the PC</p> <p style="text-align: right; color: red; font-size: x-small;"><a href="#">Learn More &gt;&gt;</a></p>

Trend Micro Channel Confidential

Mar-2008

22

Copyright 2008 - Trend Micro Inc.



# Total Web Threat Protection - Summary

Trend Micro  
Securing Your Web World



→ Malware writers are motivated by profit not fame

→ New malware is:

- Constantly changing
- Aimed to be undetectable
- Intended to reap information for profit (botnets)

→ Pattern matching is less and less viable:

- Constantly changing malware signatures
- High volume of patterns leading to HUGE pattern files
- Rate of pattern updates required is untenable

**You need total web threat protection from Trend Micro**

# Total web threat protection

Trend Micro  
Securing Your Web World

Instant  
dynamic,  
Always  
up-to-date  
protection

Available to all  
Trend Micro  
Customers

Multi-layer,  
multi-threat  
solution





**Trend Micro**

Securing Your Web World



**Trend Micro**

Securing Your Web World



**Veli-Pekka Kusmin**  
*Pre-Sales Engineer*



**TREND**  
M I C R O™

**Trend Micro Baltics & Finland**  
Pakkalakuja 7, 3<sup>rd</sup> floor  
FI-01510 Vantaa  
Finland

Telephone +358 9 4730 8300

Direct +358 9 4730 8302

Fax +358 9 4730 8999

Mobile +358 40 596 7181

[veli-pekka\\_kusmin@trendmicro.com](mailto:veli-pekka_kusmin@trendmicro.com)

<http://fi.trendmicro-europe.com>