



Securing Your Web World

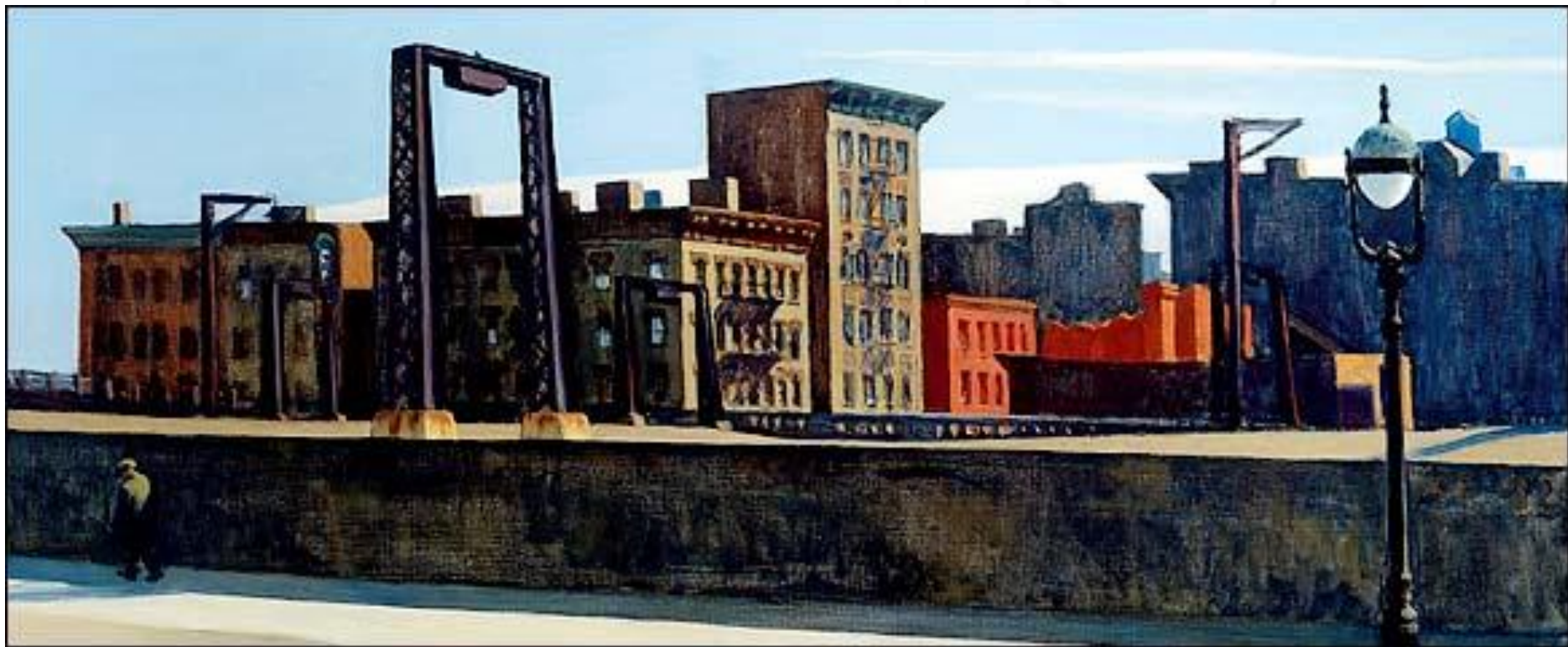
The future of Cybercrime – challenges and solutions

Panel Discussion

Alice Decker
Senior Researcher Antivirus

CoE
10th March 2009

In the past, bad guys were individuals in known bad neighborhoods



They used to code bad programs (malware) in their leisure time. That bad guys were conducting cybercrime (spreading malware) by accident or by the purpose of showing off.

Now the bad guys are next door to us



Now there's a well organized cybercrime economy where the threats are silently infecting PCs and harming people's and business' reputations and finances.

What does “infect” my Computer?



- **Malware** is any computer program that can/is used to exercise individual, collective or business harm.
 - A **Trojan** is malware that is designed/used to manipulate computer systems like stealing passwords, intercepting data, opening ports, changing system settings (hiding programs, forbid application’s execution, etc.). Trojans usually arrive as an attachment to email or as a downloaded program via the web.

E-mail



Exploited
system/application
vulnerabilities



Removable storage



The Web



What does “infect” my Computer?



- In the past **Malware** was developed for fun, to show off in communities, to highlight security issues or to combat the evil commerce.
 - A **Worm** is malware that may do all the same things a Trojan can do. Additionally a Worm replicates itself (creates copies) on disk or via network (LAN, web or email)

E-mail



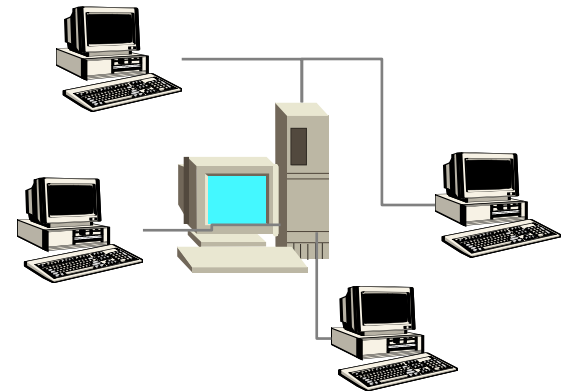
Exploited
system/application
vulnerabilities



Removable storage



The Web



What does “infect” my Computer?



- **Malware’s** applied technologies are nowadays as complex as the criminal business models.
 - A **Virus** is malware that may do all the same things a Worm can do. Additionally a Virus replicates itself in applications or data files (macro and script). They are executed when normal system programs are started.

E-mail



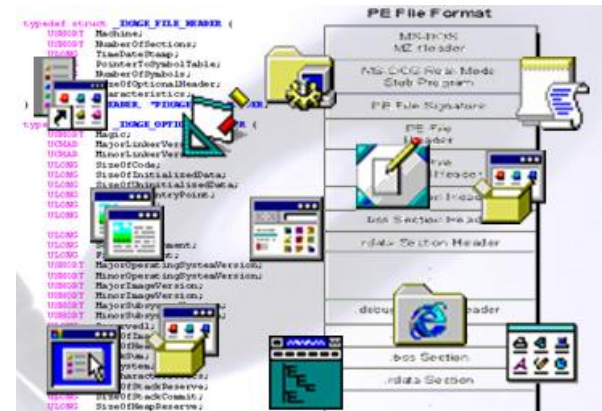
Exploited system/application vulnerabilities



Removable storage



The Web



The IT world is no longer orderly and compartmentalized



Today, network boundaries are obscured

Securing Your Web World



...

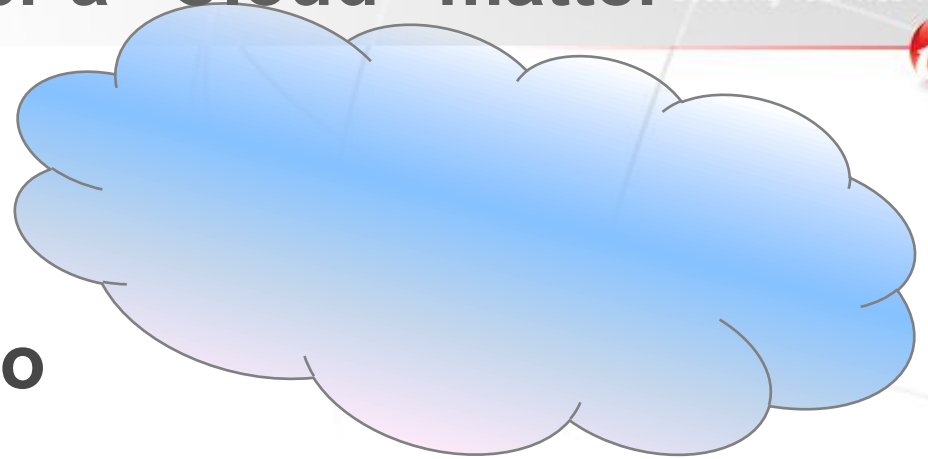


... and information transactions are easily confused



Cybercrime is no longer a “Cloud” matter

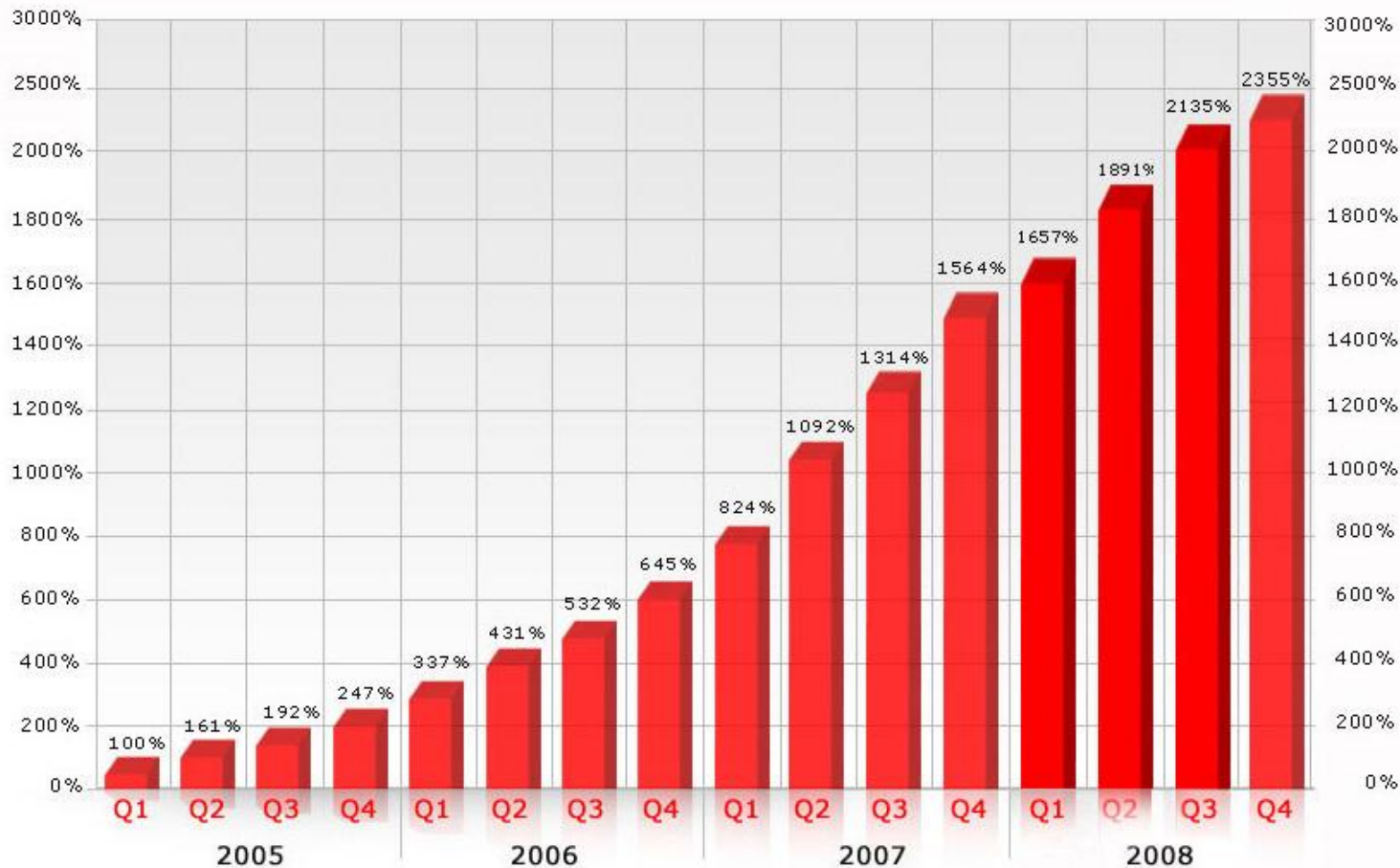
Securing Your Web World



- **Cybercrime is used to**

- Steal money
- Collect and sell data (intellectual property , industrial espionage, personal information)
- Support terrorism (attacks on SCADA, Internet or governmental infrastructure)
- Blackmail corporations, organizations and individuals

Web Threat Growth

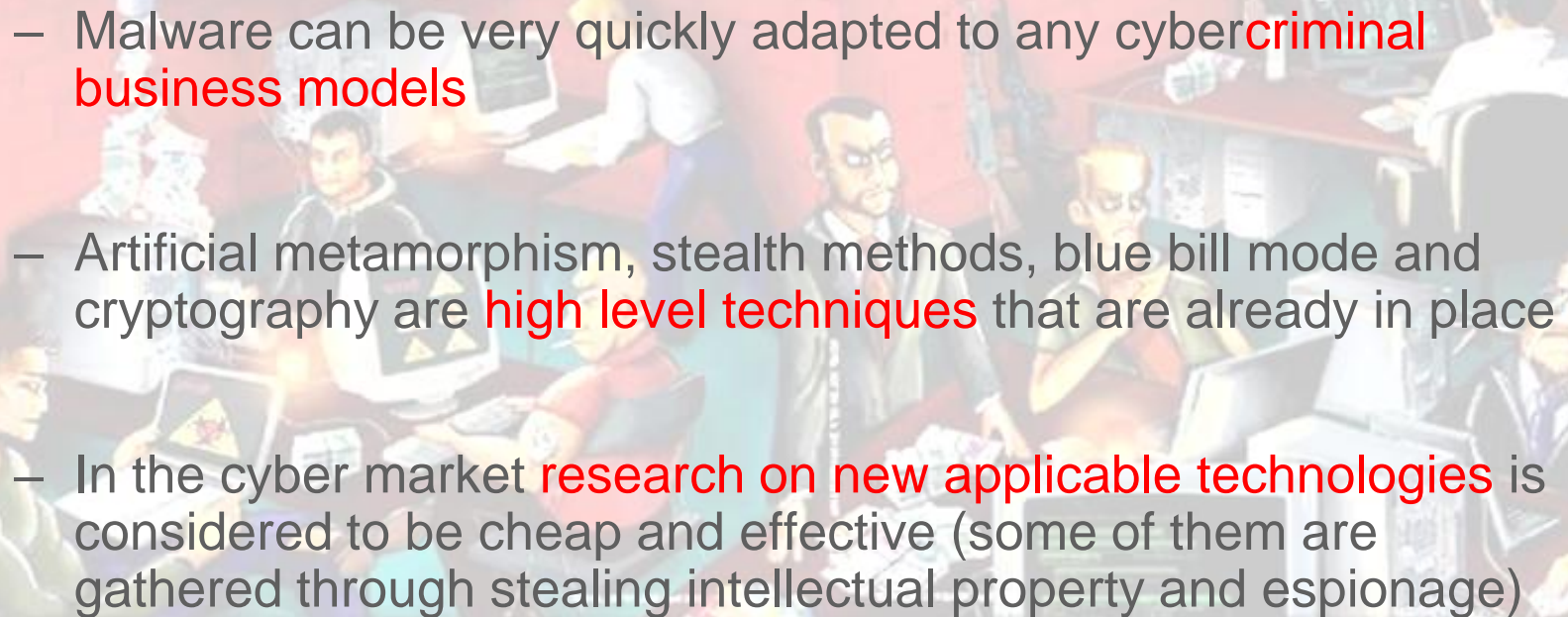


Since 2005 the number of Web threats increased with 2355%. Trend Micro receives and processes more than 15,000 unique samples per day.

The Cyber-Future ...



- ...We are right in the middle

- 
- Malware can be very quickly adapted to any cyber **criminal business models**
 - Artificial metamorphism, stealth methods, blue bill mode and cryptography are **high level techniques** that are already in place
 - In the cyber market **research on new applicable technologies** is considered to be cheap and effective (some of them are gathered through stealing intellectual property and espionage)

Trends



- Future threats are expected to be based on

Internet Infrastructure

DNS changer
SaaS (cloud computing)
Search Engines

Internet Platform

Social Networks
Virtual Worlds
Blogs, Forums, Wiki

EXPLOITATION

Automation (Mass attacks)

SQL injection
Web sites infection
Network pollution

Conveniences

In Operating Systems
End point devices

Identity theft

<http://us.trendmicro.com/us/threats/enterprise/security-library/threat-reports/index.html>

There is more than one Solution



- **Find the criminals**

- **Follow the Money**...Law Enforcement is empowered to succeed
- **Detect malware**... Security Industry has done it from the beginning

- **Prevent cybercrime**

- **Set up International laws** to oversee conduct on the Internet ... Law Enforcement is empowered to succeed
- **Apply cutting edge technologies** like Smart Protection Network ... Trend Micro Inc. is empowered to succeed in preventing malware from disturbing digital exchange of data

<http://www.trendmicro.com>

<http://ltw.trendmicro.com>



Securing Your Web World



We develop the next generation technology for preventing cyber-crime. You'll set up the cyber-rules.
Together we'll succeed!!!