NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Dr. Jean Paul Ballerini

L'Evoluzione delle Minacce in Rete

IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.
Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.

Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach

© 2008 IBM Corporation

X-Force

© 2008 IBM Corporation

Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach

© 2008 IBM Corporation

The vulnerability to malware lifecycle

Phase 1: The Vulnerability

Phase 2: The Patch

Phase 3: The Exploit

Phase 4: Malware Delivery

© 2008 IBM Corporation

2007 Vulnerability Highlights

- 6437 total vulnerabilities disclosed
- Fewer vulnerabilities were publicly disclosed in 2007 in comparison to 2006—a 5.4% decrease overall.
- Nearly 90 percent of 2007 vulnerabilities could be remotely exploited, up by 1% from 2006.
- Although total vulnerability disclosures went down, the number of reported high severity vulnerabilities increased by 28% in comparison with 2006.

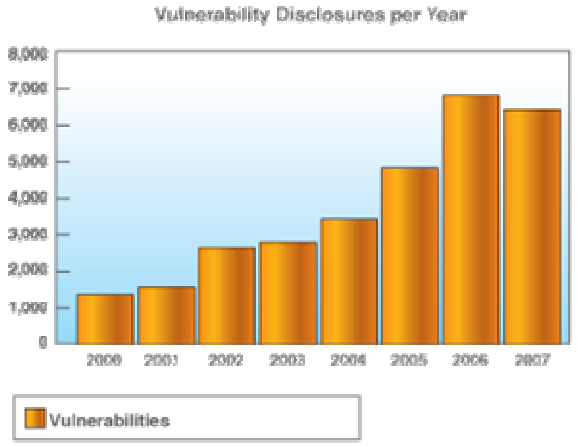


Figure 1. Total Vulnerability Disclosures from 2000 – 2007

© Copyright IBM Corporation 2008

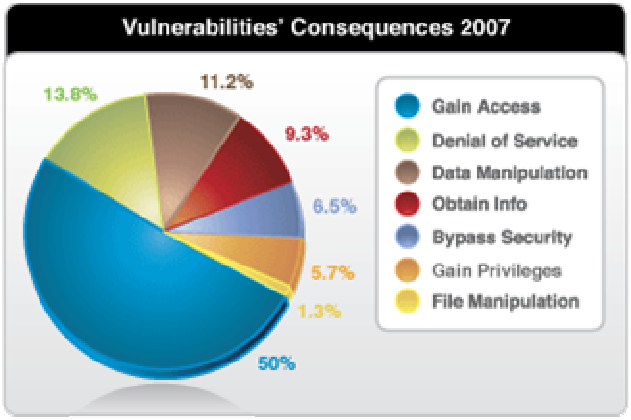


Figure 12: Vulnerabilities' Consequences in 2007

© Copyright IBM Corporation 2008

© 2008 IBM Corporation

An Attackers Perspective

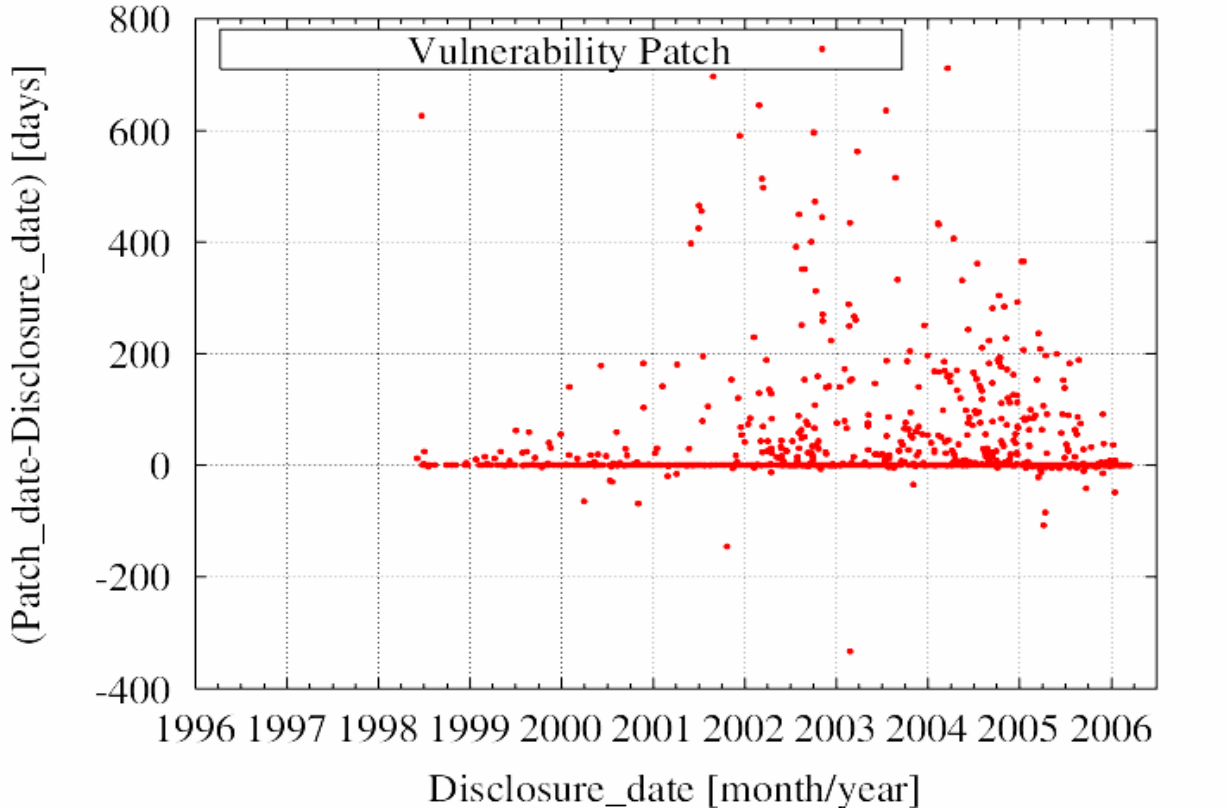
- The most valuable vulnerabilities are those that are:
  - Remotely Exploitable
  - Will allow access to the host

- In 2007:
  - Remotely Exploitable = 89.4%
  - Gain Access = 50%

- Trend is continuing towards “High Value” vulnerabilities
  - Not necessarily traditional “High Impact” vulnerabilities

© 2008 IBM Corporation

Patch Availability Date



Y-Axis

- **days between patch and disclosure date in days**

X-Axis

- **disclosure date**

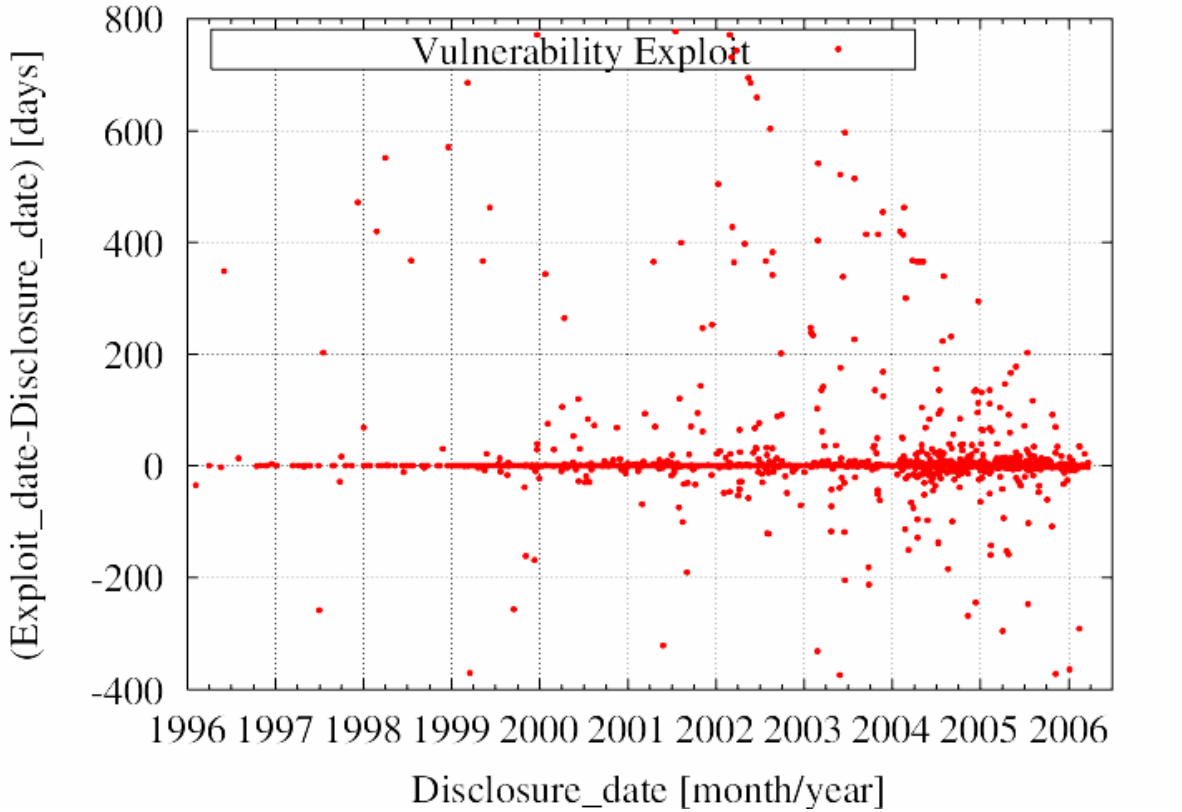
Data

- **1,551 patches**
- **15% before disclosure**
- **54% at disclosure**
- **31% after disclosure**

Courtesy: Stefan Frei, ETH Zurich – http://www.techzoom.net/risk/

© 2008 IBM Corporation

Exploit Availability Date



Y-Axis

- **days between exploit and disclosure date in days**

X-Axis

- **disclosure date**

Data

- **3,428 exploits**
- **23% before disclosure**
- **58% at disclosure**
- **19% after disclosure**

Courtesy: Stefan Frei, ETH Zurich – http://www.techzoom.net/risk/

© 2008 IBM Corporation

Patch to Exploit

- Legitimization of reverse engineering and exploit development
- Freeware tools promote ‘kudos’ and legitimacy framework to exploit release
  - Metasploit project
- Commercial groups focus on developing exploits for patched vulnerabilities
  - Vulnerability scanners
  - Protection reviews
  - “Weaponization” contracts
  - False negative/positive reduction

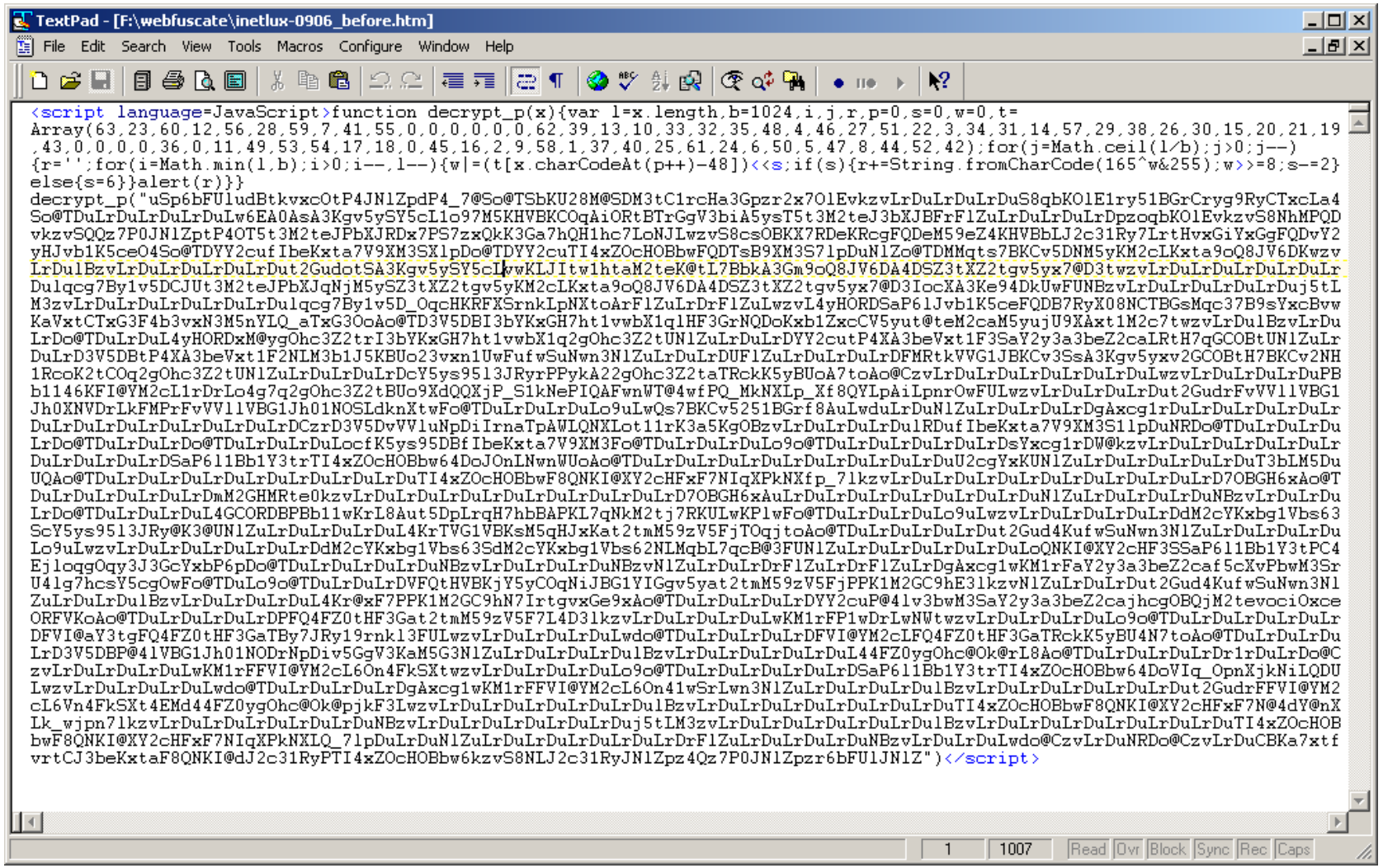
© 2008 IBM Corporation

Providers - Inet-lux

- WebAttacker Toolkit
  - DIY malware creation kit, less than $20
- Framework for distributing and using new exploits
  - Cycle through vulnerabilities until one works
- “Managed Exploit Providers”

DON’T GO TO THEIR WEBSITE!

© 2008 IBM Corporation



© 2008 IBM Corporation

2007 Malcode Highlights

- X-Force collected and analyzed nearly 410,000 new malware samples in 2007, almost a third more than it researched in 2006.
- Trojans represent the largest category of malware in 2007—109,246 varieties account for 26% of all malware.
- The most frequently occurring malware on the Internet was Trojan.Win32.Agent— 26,573 varieties in 2007 account for 24% of all Trojans.
- The most common worm in 2007 was Net-Worm.Win32.Allaple with 21,254 varieties. It is a family of polymorphic worm that propagates by exploiting Windows® vulnerabilities instead of using e-mail.

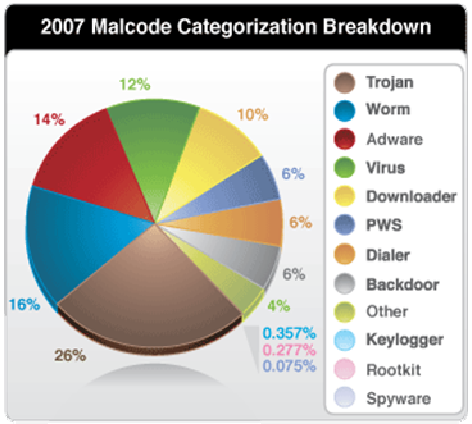


Figure 29: 2007 Malcode Characterization Breakdown

© Copyright IBM Corporation 2008

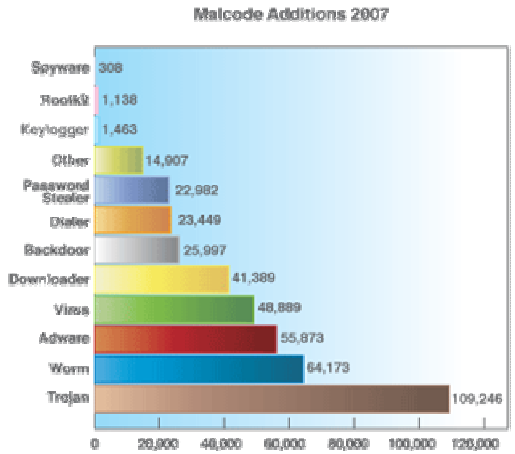


Figure 31: 2007 Malcode Additions

© Copyright IBM Corporation 2008

© 2008 IBM Corporation

Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

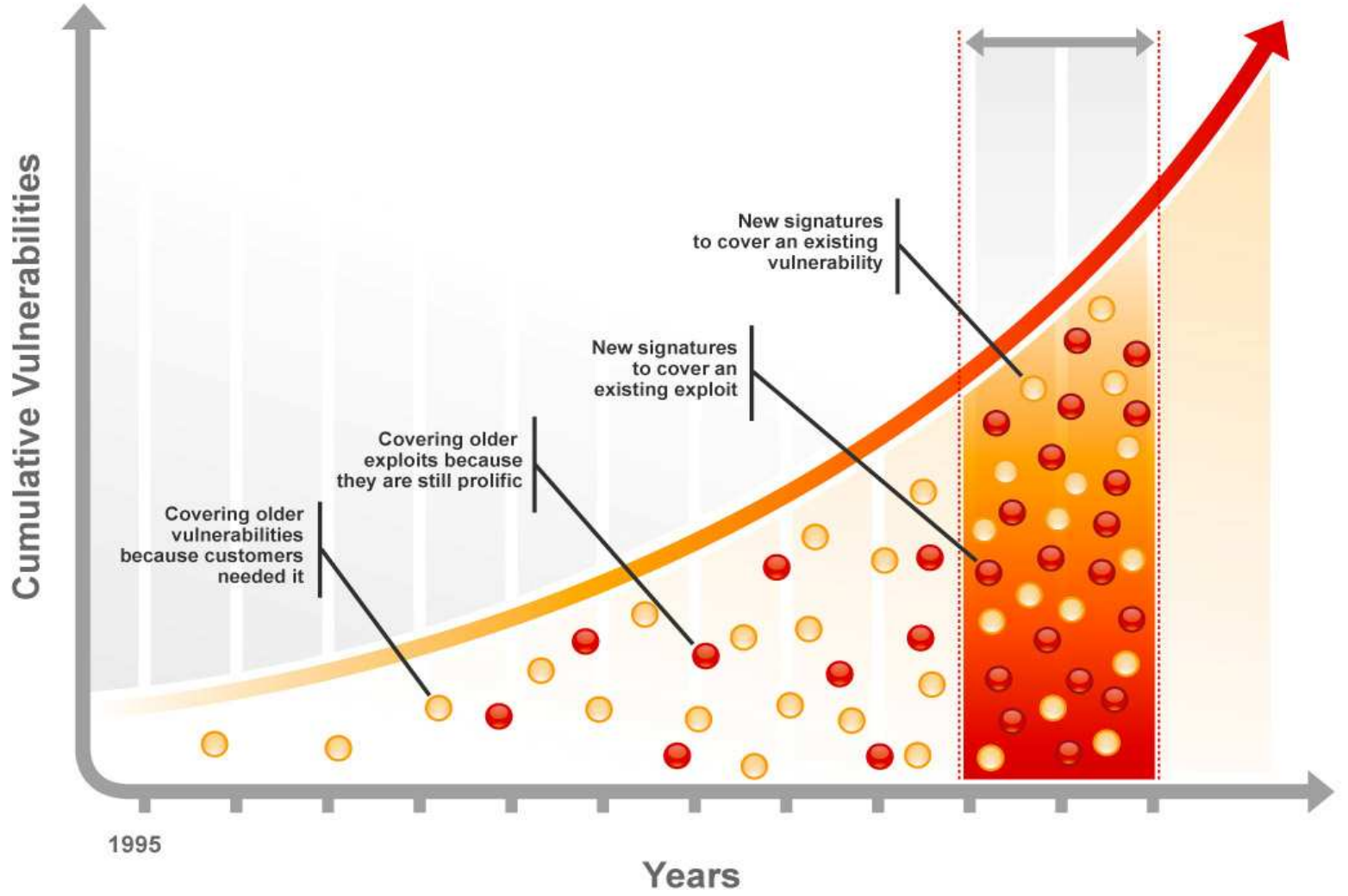
IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach

© 2008 IBM Corporation

NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

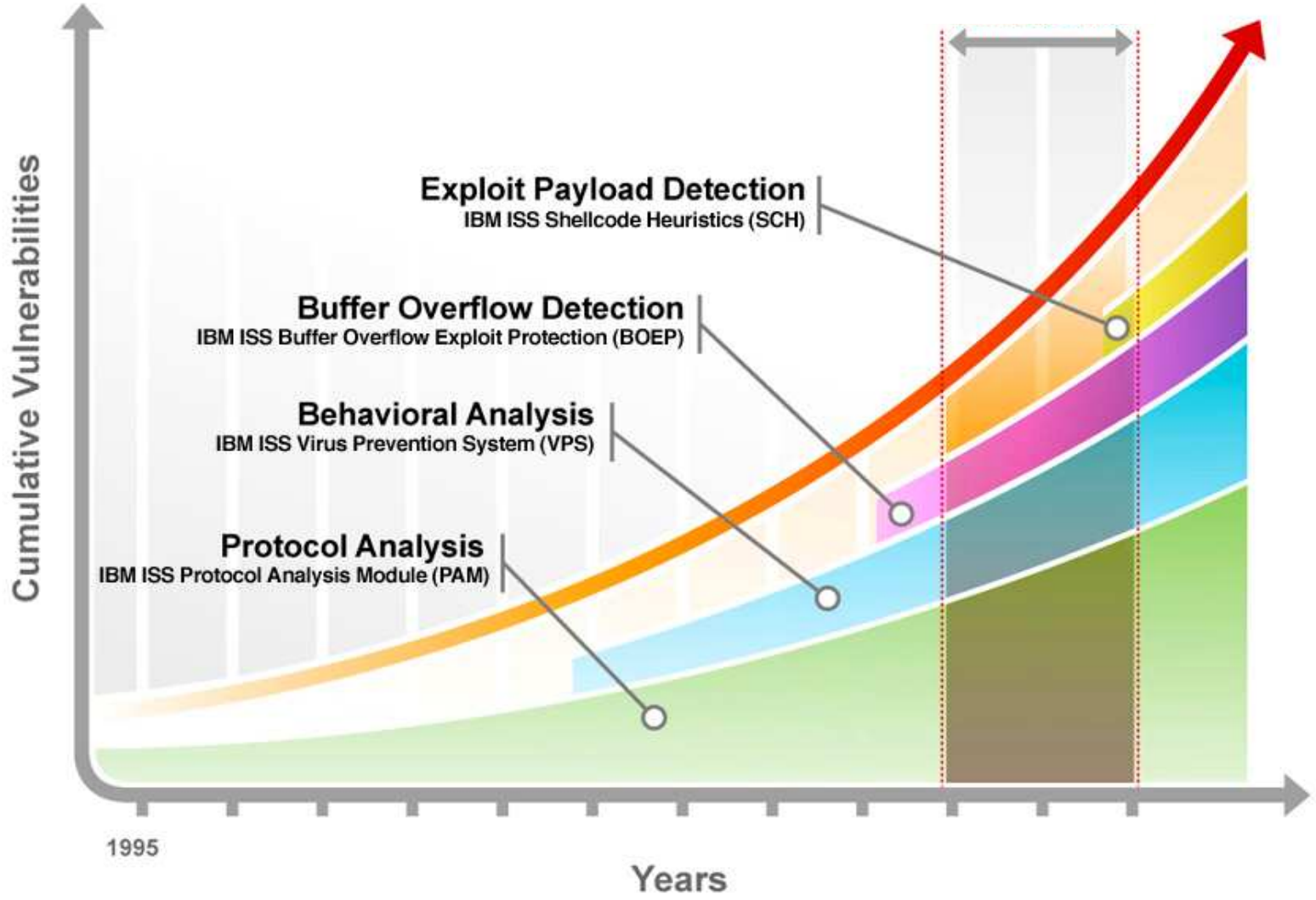
IBM



BASTA PARLARE **INIZIAMO A FARE**

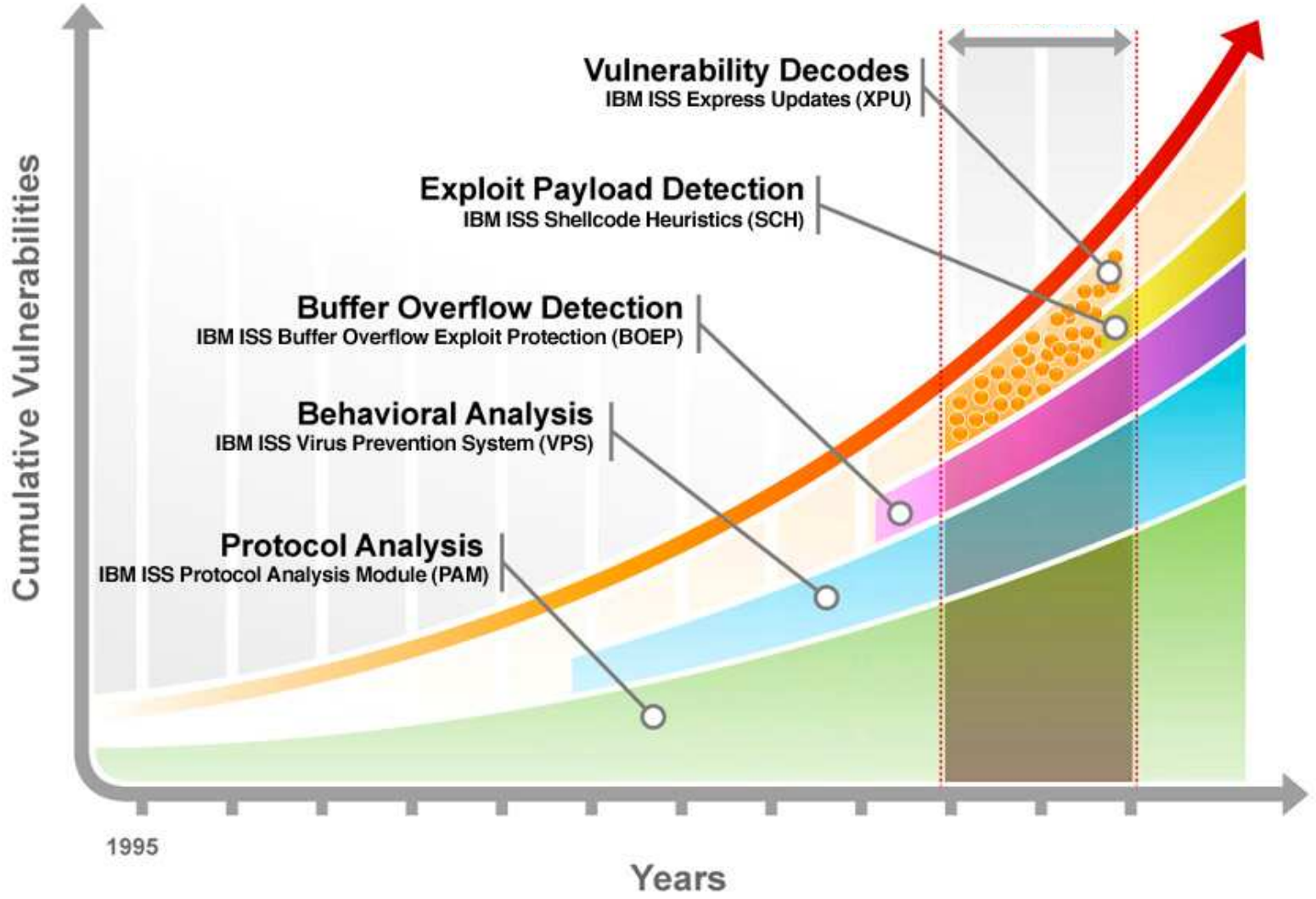
© 2008 IBM Corporation

ISS Preemptive Protection



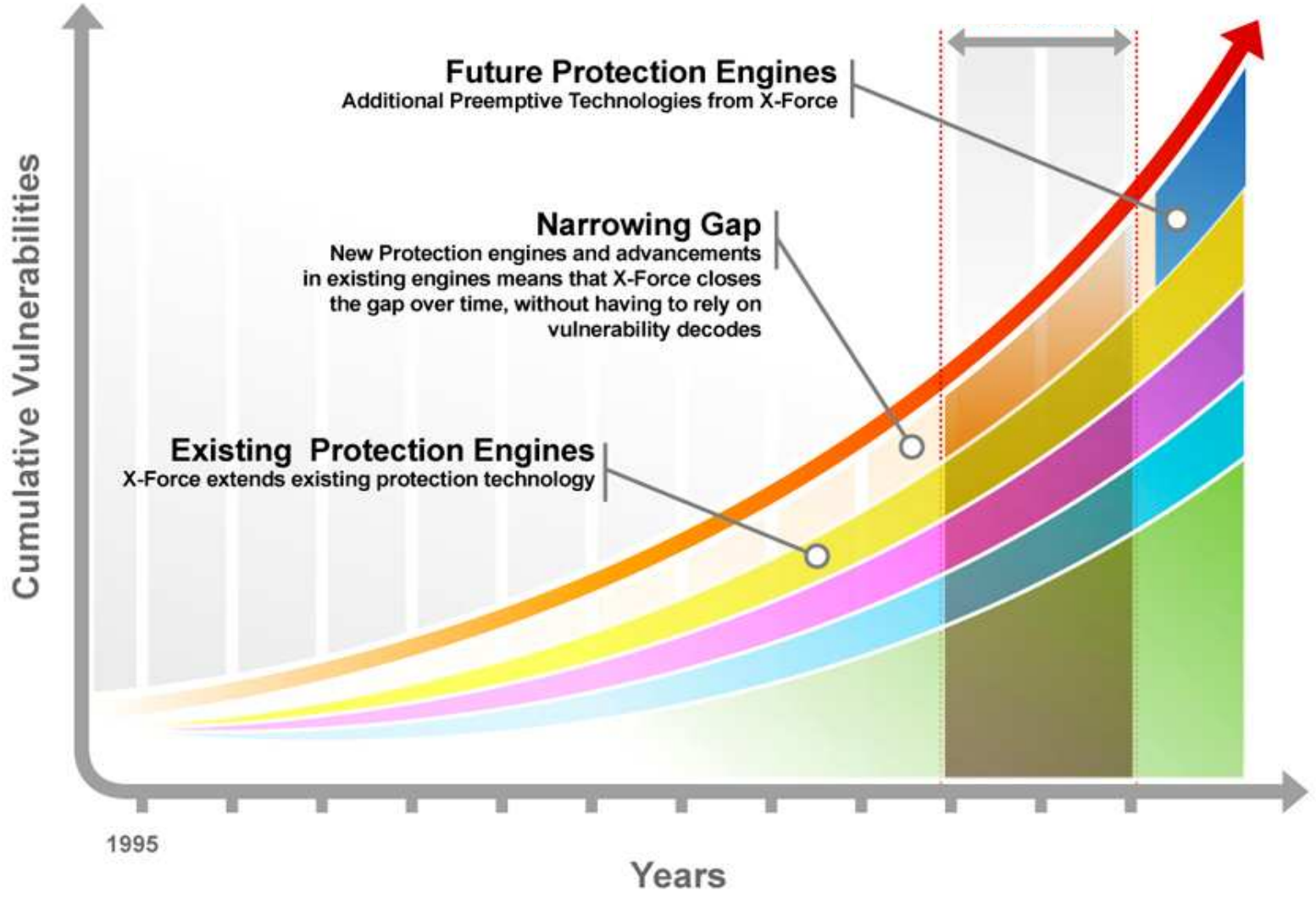
© 2008 IBM Corporation

Vulnerability Focused Protection



© 2008 IBM Corporation

Protection Advances



© 2008 IBM Corporation

How do you get “owned” these days?

The initial culprits in owning a system can be as innocent as an email from Mom or as malicious as a hacker set to steal valuable information.

SPAM

WEB

“Look at this cute dancing kitten e-card, dear!”

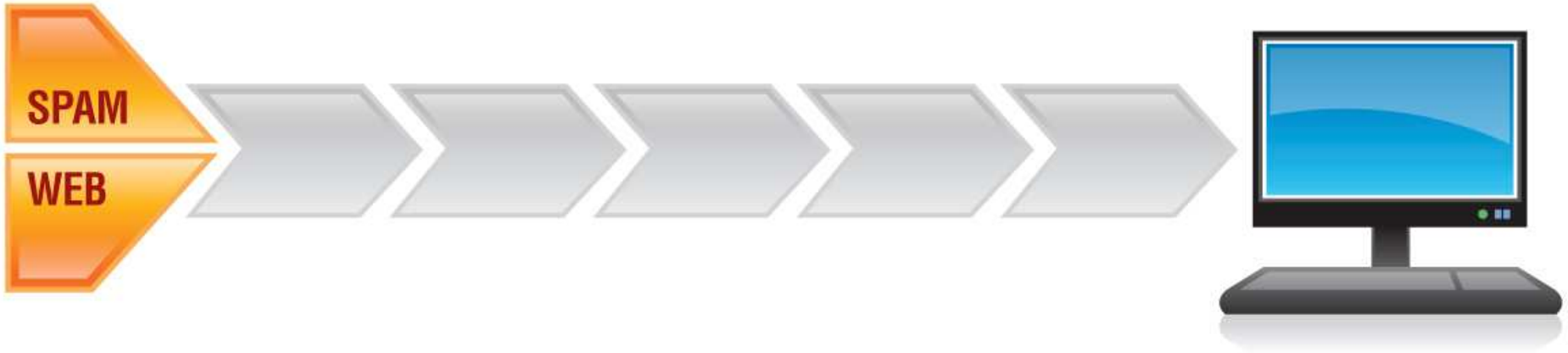
“I need money for a Wii.”

“I wonder if that stock tip I just got in my email is any good.”

© 2008 IBM Corporation

The Threat Lifecycle

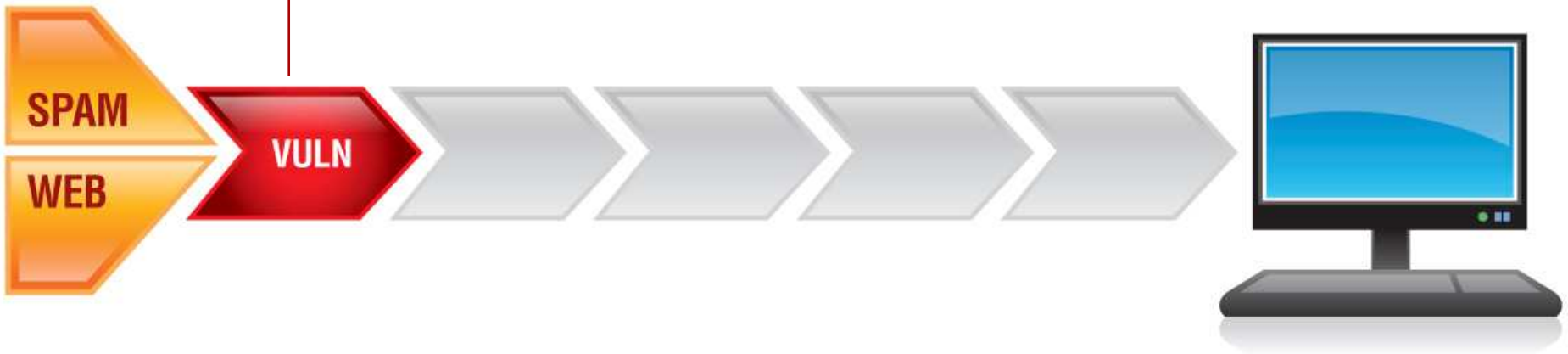
The initial culprits in owning a system can be as innocent as an email from Mom or as malicious as a hacker set to steal valuable information.



© 2008 IBM Corporation

The Threat Lifecycle

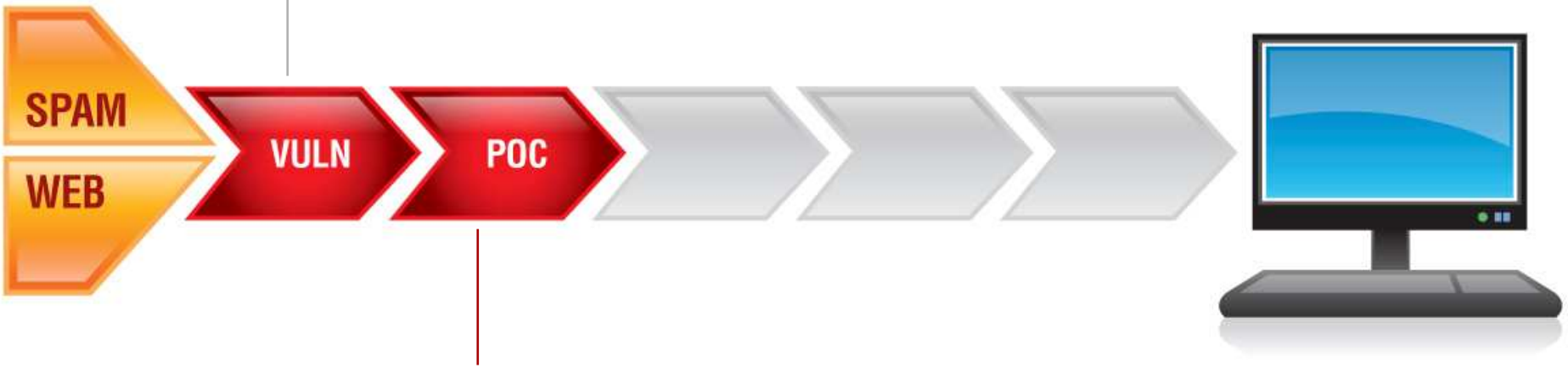
Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.



© 2008 IBM Corporation

The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.



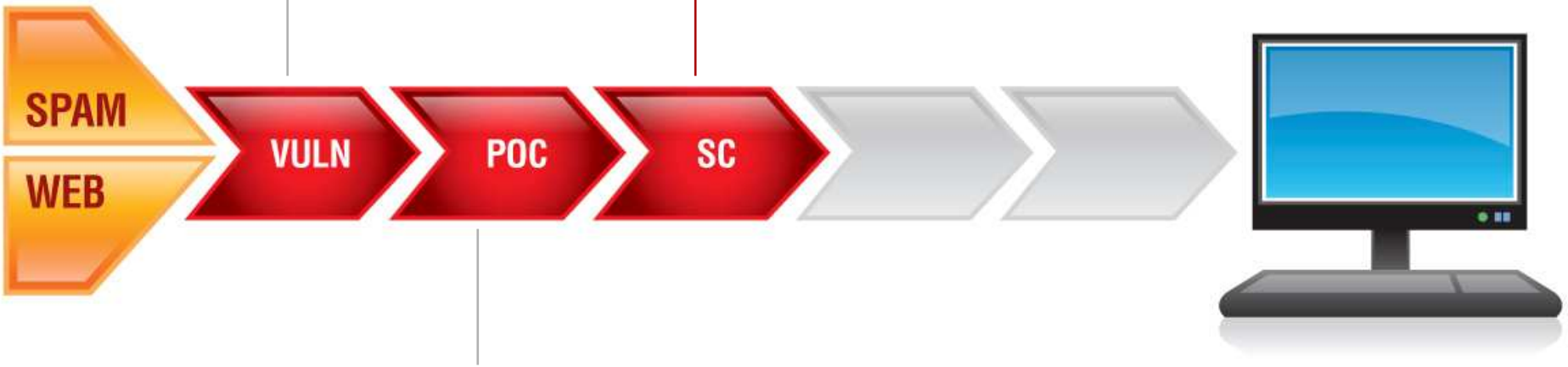
A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability

© 2008 IBM Corporation

The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution



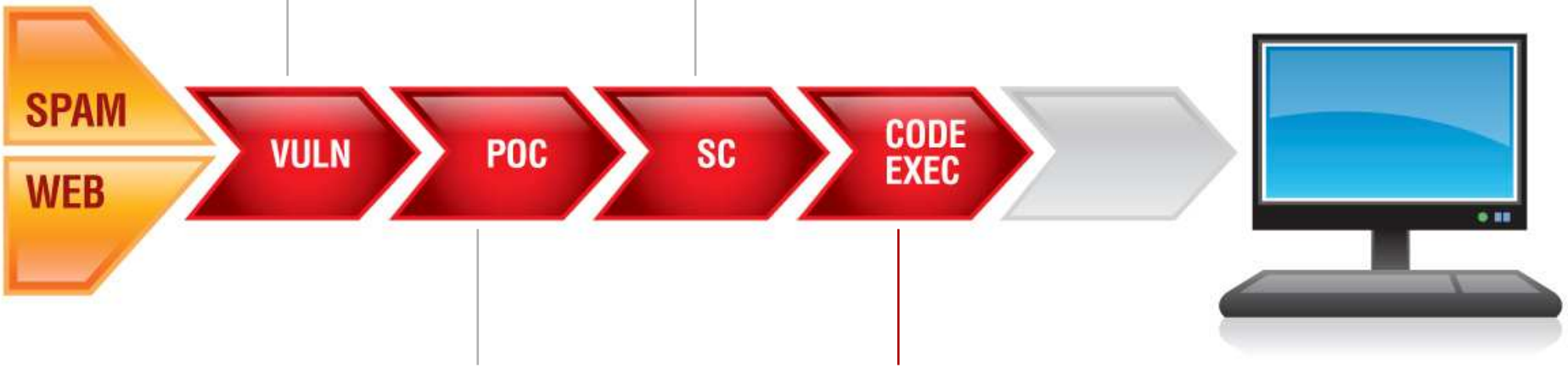
A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability

© 2008 IBM Corporation

The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution



A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability

Shell code is executed to create a buffer overflow that opens the back door to the system

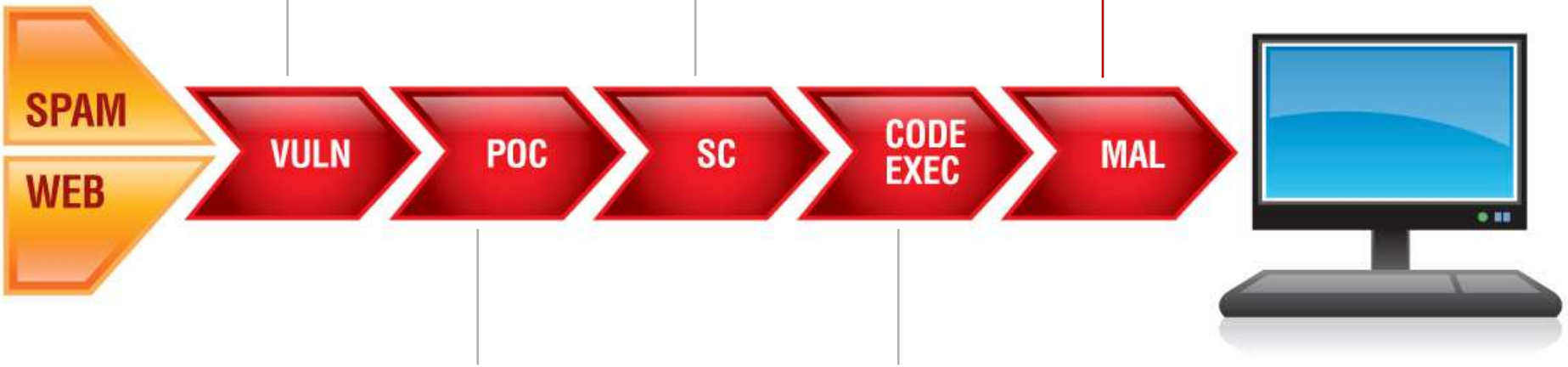
© 2008 IBM Corporation

The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution

Malcode, such as a trojan or rootkit is executed to wreak havoc on the system



A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability

Shell code is executed to create a buffer overflow that opens the back door to the system

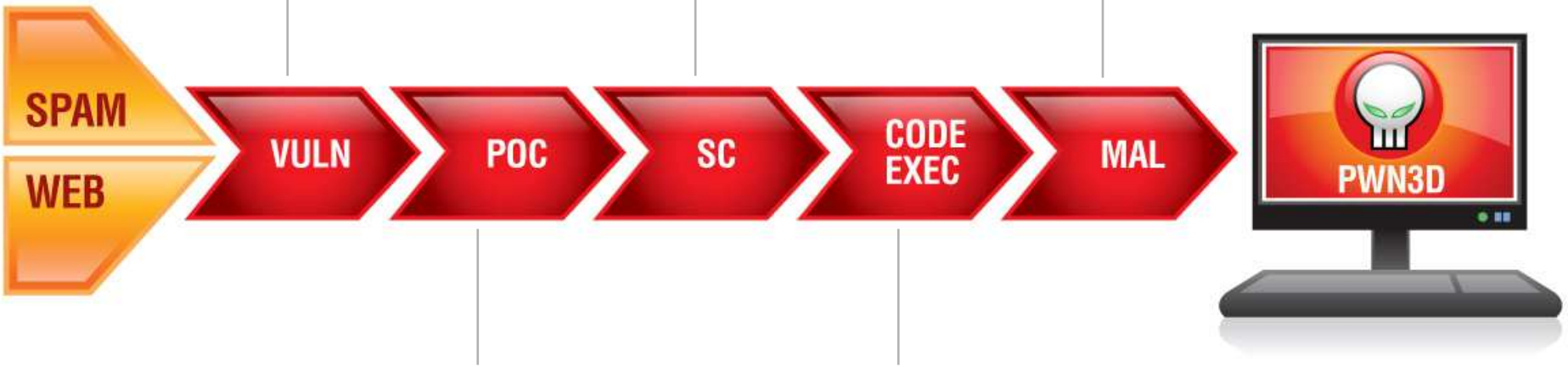
© 2008 IBM Corporation

The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution

Malcode, such as a trojan or rootkit is executed to wreak havoc on the system



A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability

Shell code is executed to create a buffer overflow that opens the back door to the system

© 2008 IBM Corporation

X-Force Protection Engines

Cobion

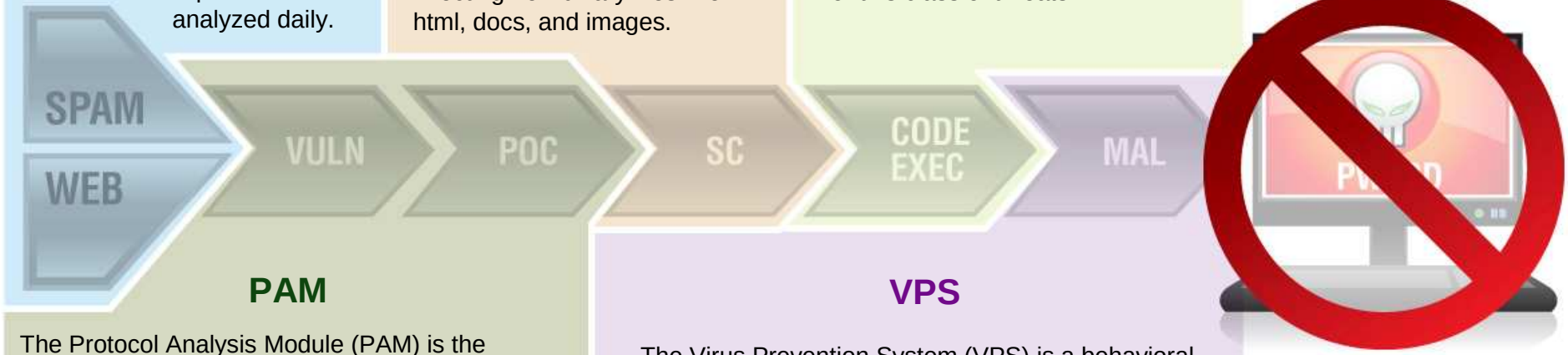
Cobion e-mail and content filtering technology has analyzed over 8.7B URLs and images and 1B unique spam messages. Over 100k web/700k spams analyzed daily.

Shellcode Heuristics

This engine uses generic shellcode detection to block shellcode payloads, one of the most prevalent method of infecting non-binary files like html, docs, and images.

BOEP

Buffer Overflow Exploit Prevention (BOEP) blocks execution payloads delivered through buffer overflow exploits, providing 0-day protection for this class of threats.



PAM

The Protocol Analysis Module (PAM) is the network IPS component in IBM ISS desktop, server, and network products. PAM uses behavioral and vulnerability-centric methods to detect and block network-based exploits affecting more than 7,400 vulnerabilities.

VPS

The Virus Prevention System (VPS) is a behavioral anti-virus technology that can stop not only new malware variants, but also new malware families. VPS uses pre-execution behavioral analysis to stop malware before it can run and do damage.

© 2008 IBM Corporation

Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach

© 2008 IBM Corporation

X-Force R&D Drives IBM ISS Security Innovation

Research → Technology → Solutions

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

© 2008 IBM Corporation

NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Questions?

Thank you!

Dr. Jean Paul Ballerini

jpballerini@it.ibm.com

IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.
Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.