Fixing the Fundamental Failures of End-Point Security

Managing vulnerabilities when perimeter protection has failed

Dr. Stefan Frei
Research Analyst Director

Mail: sfrei@secunia.com
Twitter: @stefan_frei

Agenda

- The Changing Threat Environment
- Live demo with Malware Construction Kit
- Complexity of End-Points
  (or the Easy Prey for Cyber Criminals)
- Protective Measures when the Perimeter Failed

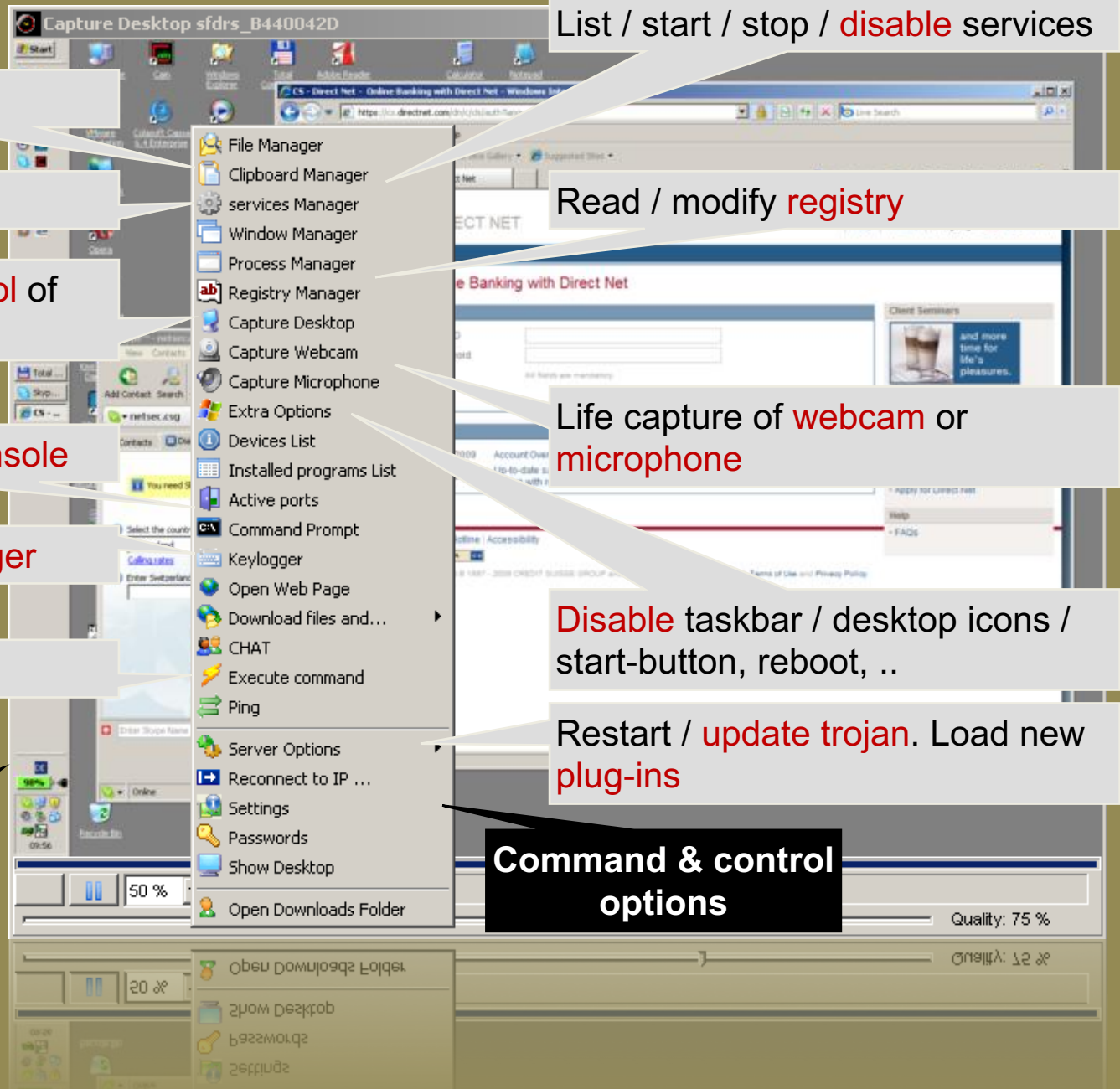
Malware Construction Kit
Live Demonstration

- Malware Construction Kit
  - We “trojanize” **Windows Minesweeper** using an off-the-shelf malware construction kit
  - No coding expertise needed

- Remote Control Capabilities
  - We demonstrate the Trojans remote management capabilities on a compromised Netbook

Malware Construction Kit

Live Demonstration



Read clipboard

List and kill processes

Life capture and control of desktop

Remote command console

Online / offline keylogger

Execute commands

List / start / stop / disable services

Read / modify registry

Life capture of webcam or microphone

Disable taskbar / desktop icons / start-button, reboot, ..

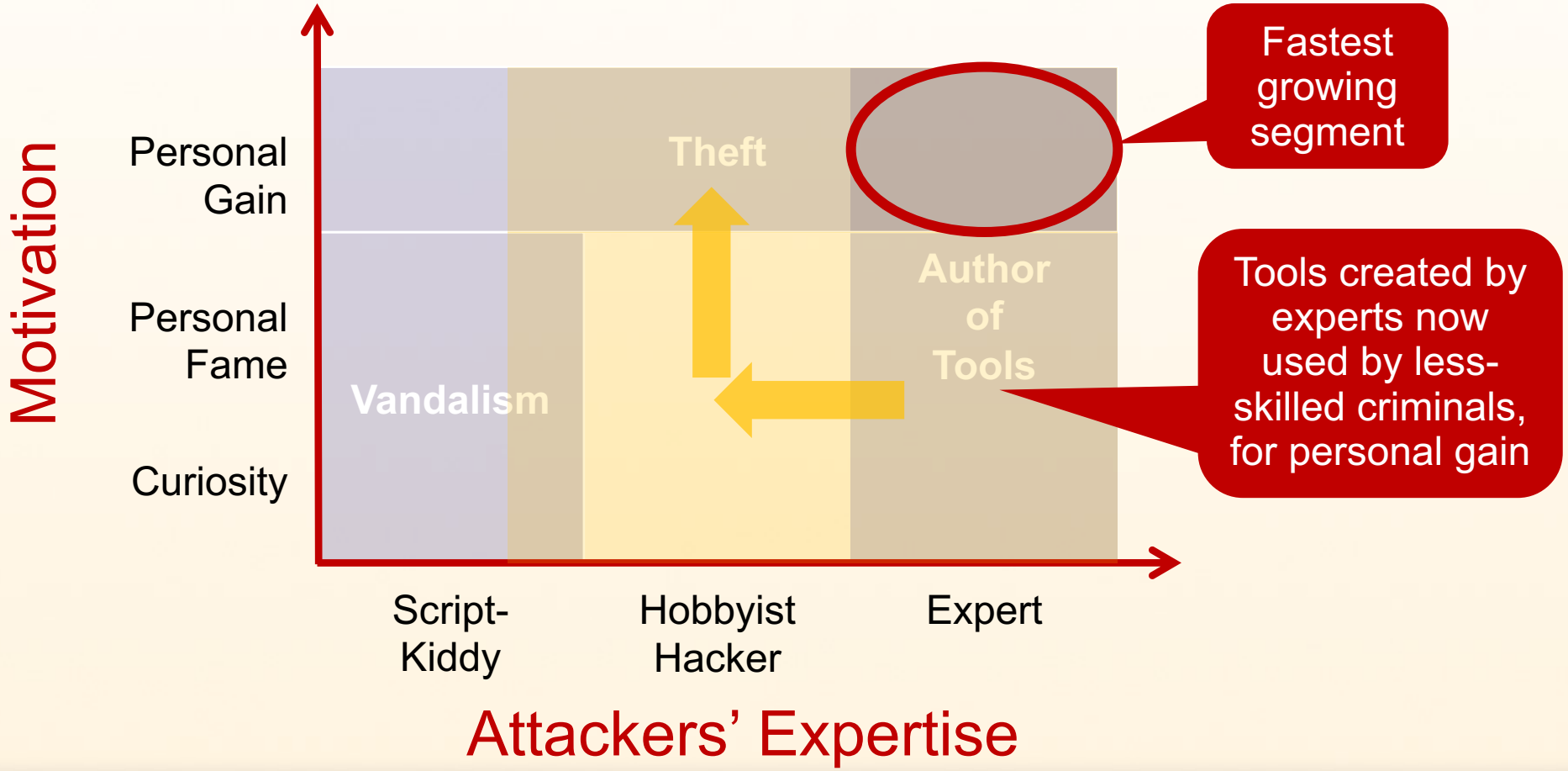
Restart / update trojan. Load new plug-ins

Life remote target session

Command & control options

The Changing Threat Environment

Motivation vs. Expertise

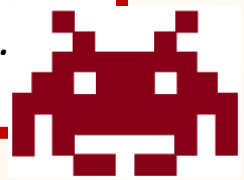


Malware Development Process

Obfuscation and Quality Assurance

1 Original Malware

Create core malicious functionality:
DDoS, steal data, spread infection, ..



2 Permutations

Obfuscate malware. Create multiple serial **variants** to thwart detection engines

3 Quality Assurance

Test new creations against a number of up-to-date anti-virus engines

4 Deployment

Only malware that passed QA (not detected) is used for deployment

Reject if detected by anti-virus

Image: www.swisscyberstorm.com
Source: Damballa http://bit.ly/SerVar

Malware Development Process

Obfuscation and Quality Assurance

A Numbers Game (2010)

~ 286 Million virus samples catalogued

~ 4,000 vulnerabilities disclosed

~ 2,000 vulns. for MS platform

100,000+ samples/vulnerability

engines

deployment

Source: Damballa http://bit.ly/SerVar

Cybercriminals' Attack Tactics

- Multiple variants of a particular malware agent are automatically created in advance of the attack:
  - Only variants that pass quality assurance (= bypass anti-virus) are used for attacks
  - Each new variant is released at scheduled intervals to constantly remain ahead of anti-virus protection updates

Malware is prevalent and can be produced to successfully bypass traditional perimeter defenses

Limitations of Traditional Protection

25% of publicly known exploits **missed** by prevention software

40% missed **after slight tweaking** of the exploit

- Up to 9% of the end-points in enterprises are found to be infected
- Cybercriminals have between 25%-97% chance of getting past consumer anti-virus

(1) Damballa on Darkreading http://bit.ly/EntBot,
(2) NSS Anti-Malware Group Test Report 2010/Q3

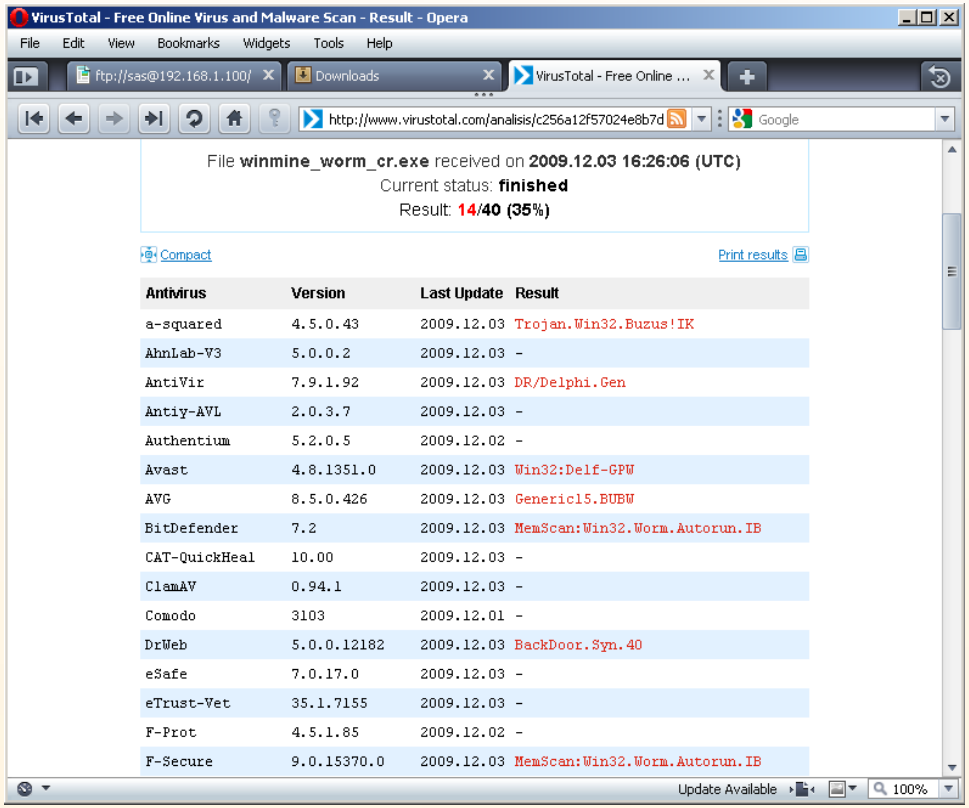
Image: www.swisscyberstorm.com
Source: Forbes - http://bit.ly/f3M1xS

Malware Construction Kit
Detection Evasion Results

Anti-virus detection before/after obfuscation of the Minesweeper Trojan used in demonstration

At the time of testing the malware kit used was more than 6 months old

Anti-Virus Detection Rate		
Date	Raw	Obfuscated
2009-12-03	77%	35%
2009-12-17		61%



Detection Tool: http://www.virustotal.com

Malware as a Service

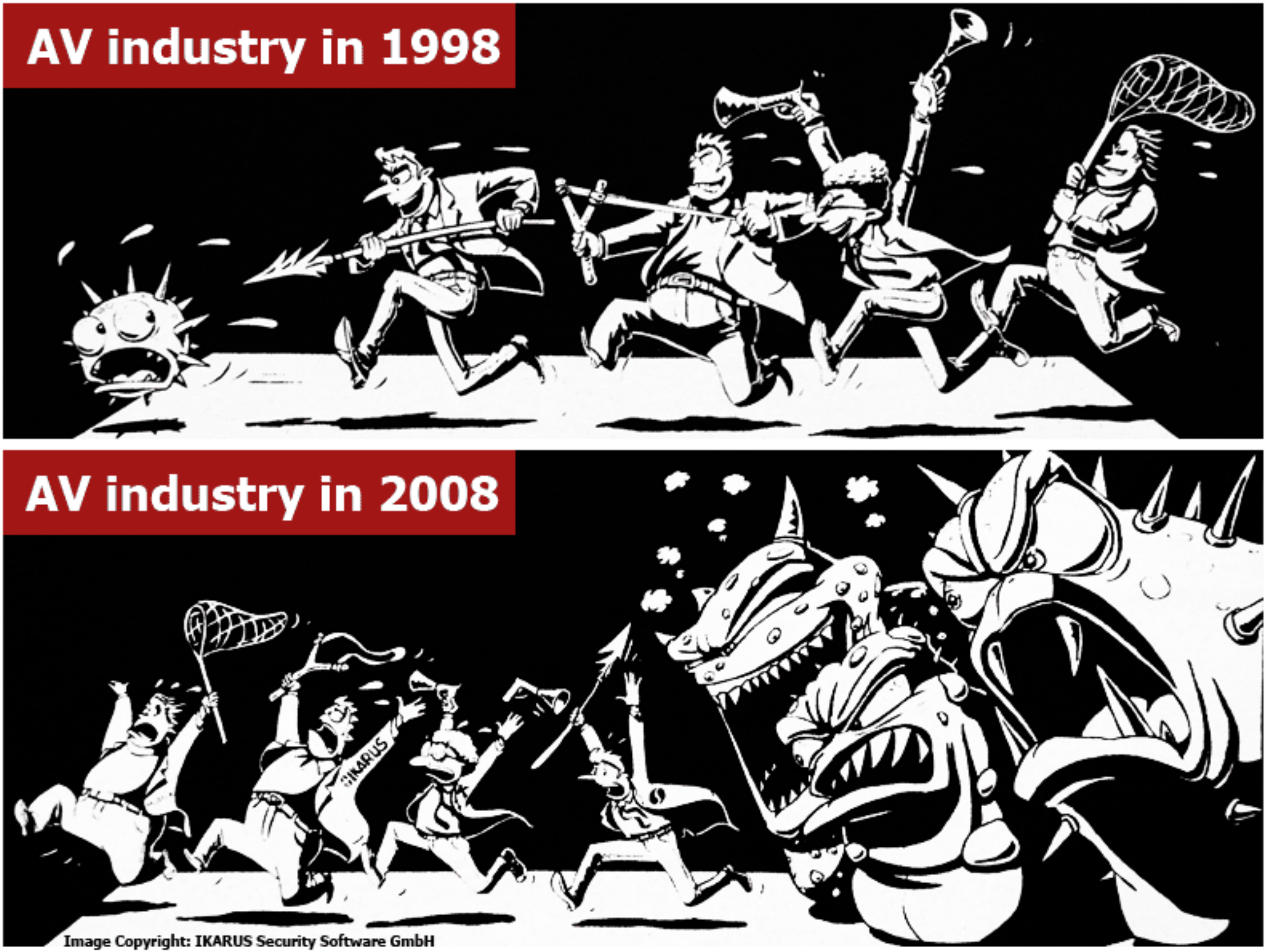
Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant mess
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249$ (United State Dollar)

Malware offered for **$249** with a Service Level Agreement and **replacement warranty** if the creation **is detected by any anti-virus** within 9 months

Source: www.turkojan.com


AV industry in 1998
AV industry in 2008
IKARUS
Image Copyright: IKARUS Security Software GmbH

Cybercrime – it's all about Profits

Tools

Tools are created by experts and used by less-skilled attackers

Attacks

More opportunistic and highly automated attacks

What is the potential, what are the preferred targets of this model?

From a Criminal's Perspective

#Hosts x #Vulnerabilities

=

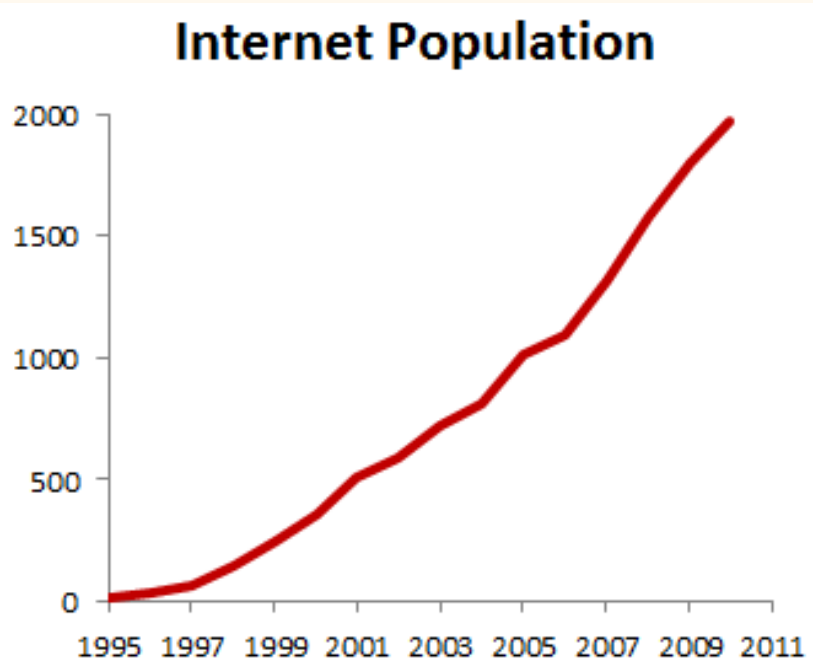
Opportunity

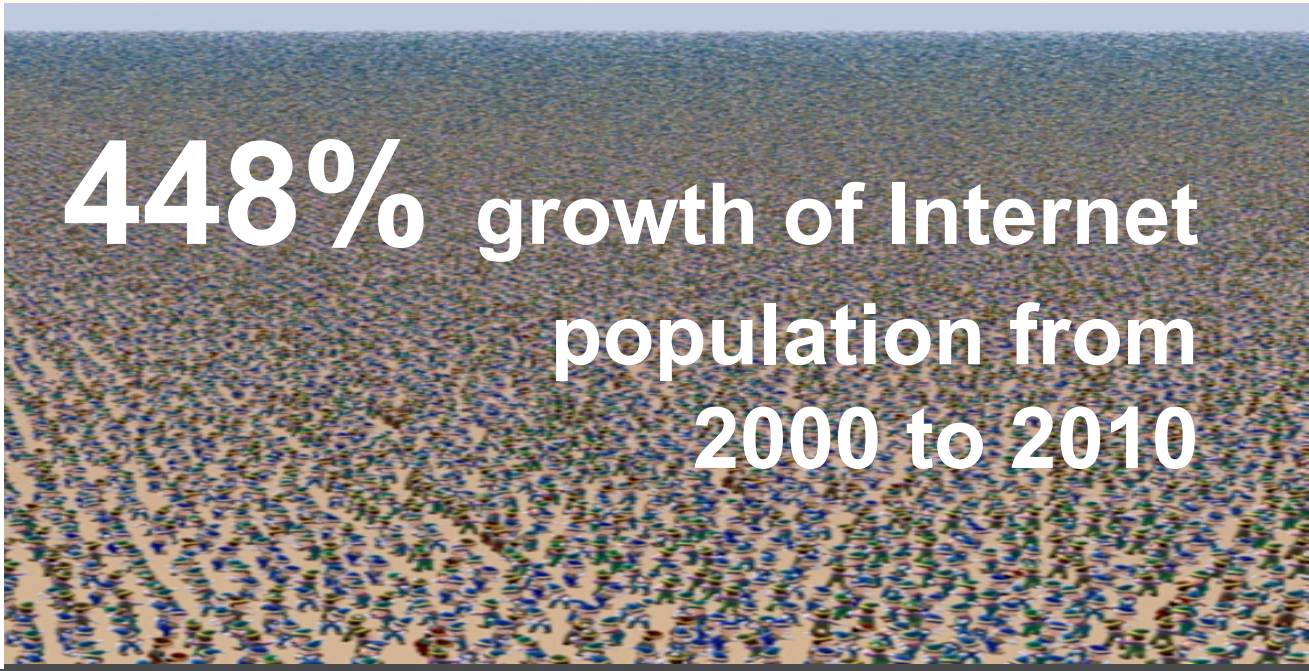
Worldwide Internet Usage

1,966 Million

estimated Internet users on 31st December, 2010

28% penetration of population





Source: Internet World Stats http://www.internetworldstats.com

1,966 Million Potential Targets ...

Corporate as well as private end-points are increasingly targeted

- End-points are difficult to secure
  - Highly dynamic environment and unpredictable usage patterns by users
- End-point PCs are where the most valuable data is found to be the least protected
  - By definition, end-point PCs have access to all data needed to conduct their business

Everyone is a valuable target for cybercriminals

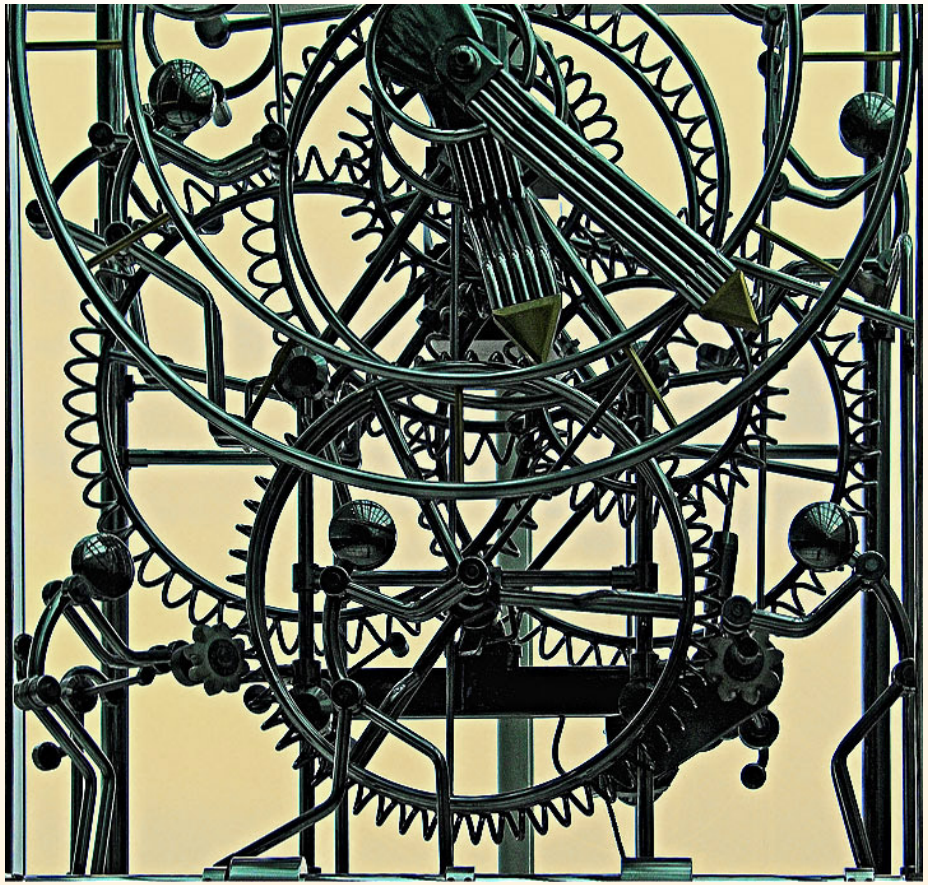
#Hosts x #Vulnerabilities

=

Opportunity

What does a typical End-Point look like?

.. numerous programs and plug-ins!

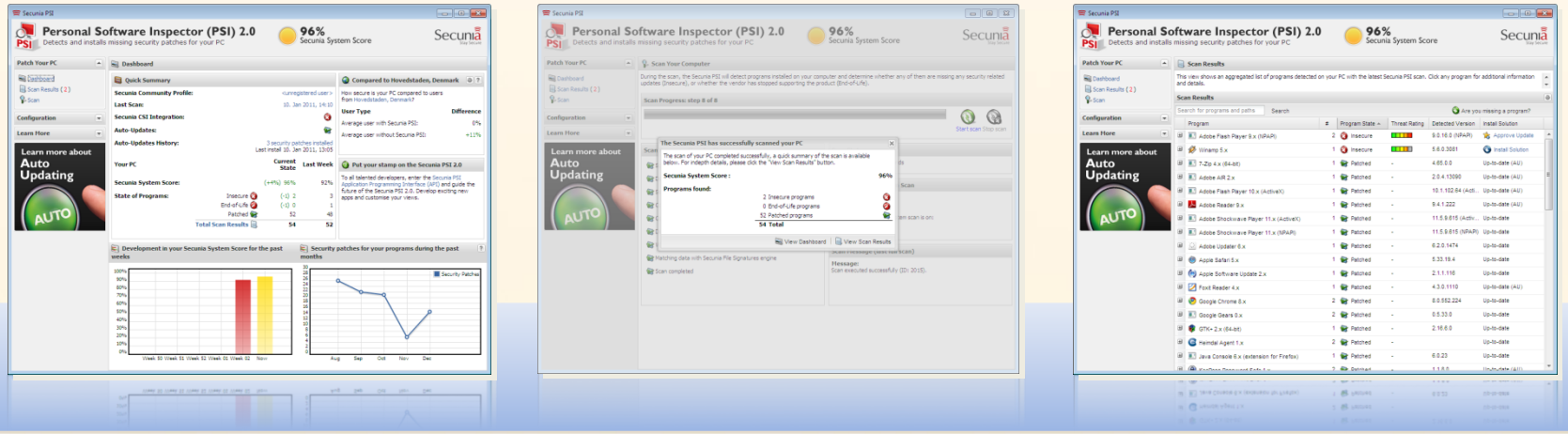


How many programs do you think you have installed on your typical Windows machine?

How many different update mechanisms do you need to keep this PC up-to-date?

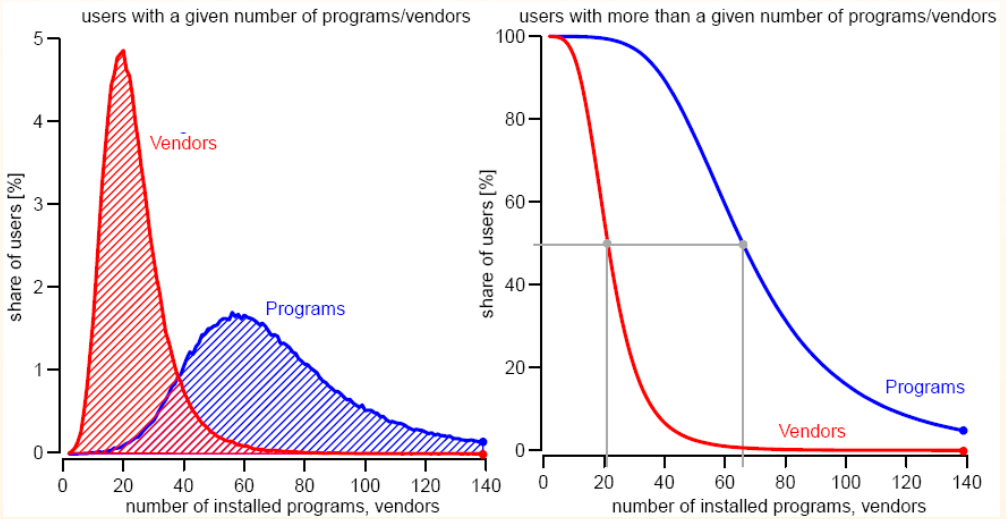
Data from Real End-Points in the Field

- Scan results from more than 3 Mio PSI users
  - Secunia Personal Software Inspector (PSI)
  - Free for personal use http://secunia.com/psi
- A lightweight software inspector/scanner to:
  - Identify insecure programs and plug-ins
  - Automatically install missing patches



Software Portfolios …

What programs do users typically have installed on their end-point PCs?



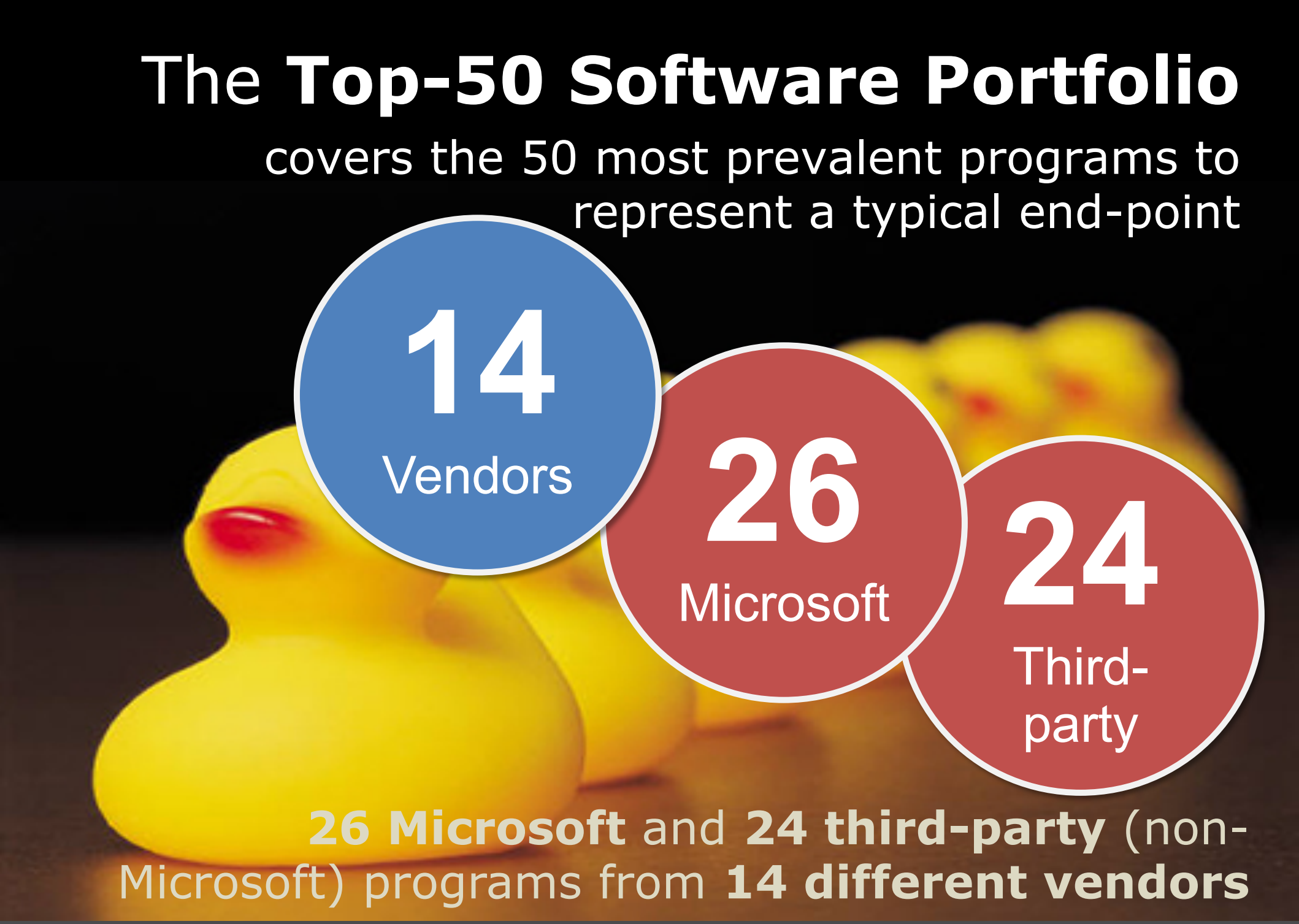
50% of users

- have more than **66 programs**
- from more than **22 vendors** installed

Analysis based on Secunia PSI scans in 2010

The **Top-50 Software Portfolio**

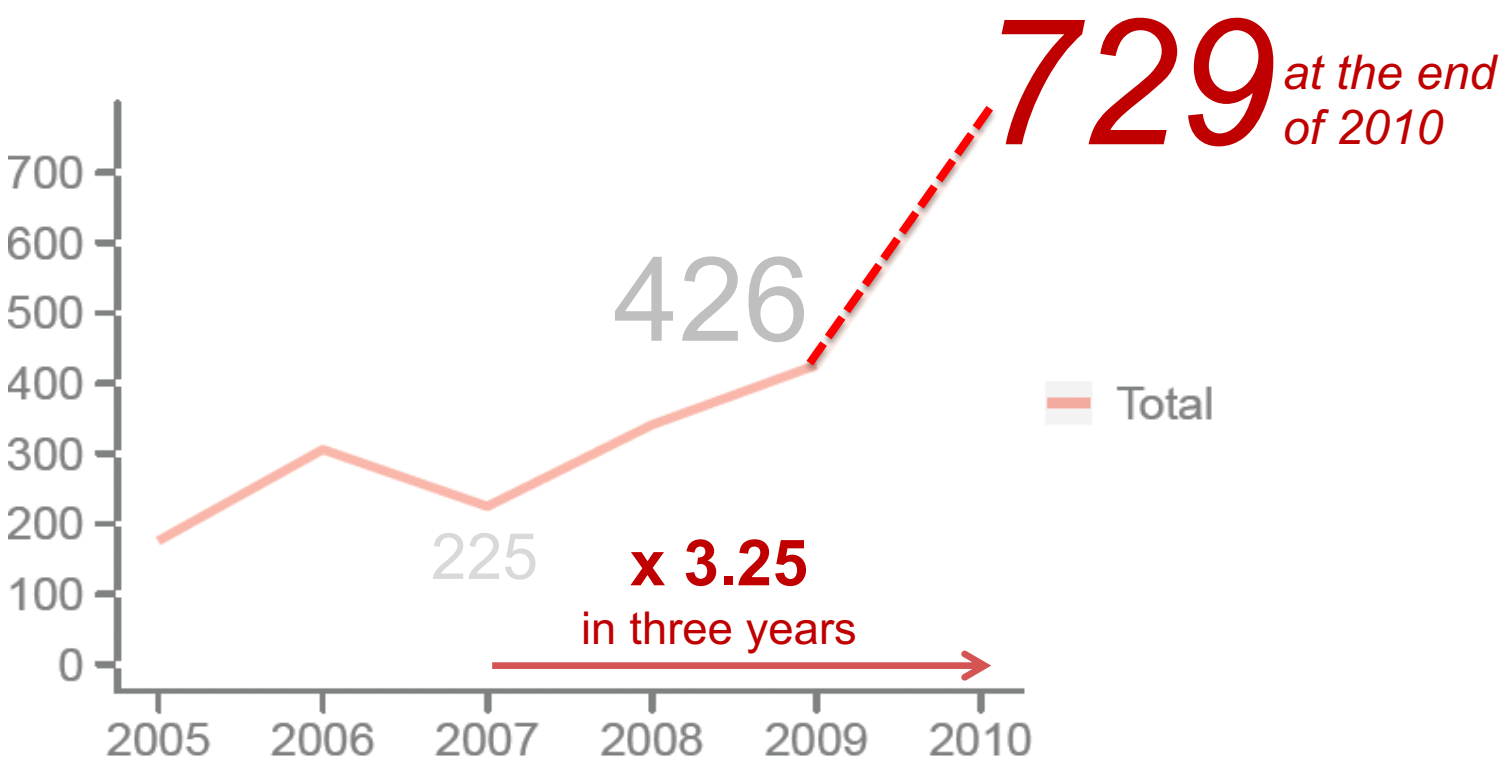
covers the 50 most prevalent programs to represent a typical end-point



26 Microsoft and **24 third-party** (non-Microsoft) programs from **14 different vendors**

An Alarming Trend …

From 2009 to 2010 alone: 71% increase



An Alarming and Relevant Trend …

More than

50% of these vulnerabilities:

- >95% are exploitable from remote
- >70% are rated as 'Highly' or 'Extremely critical'
- >50% provide system access

Source: Secunia Yearly Report 2010

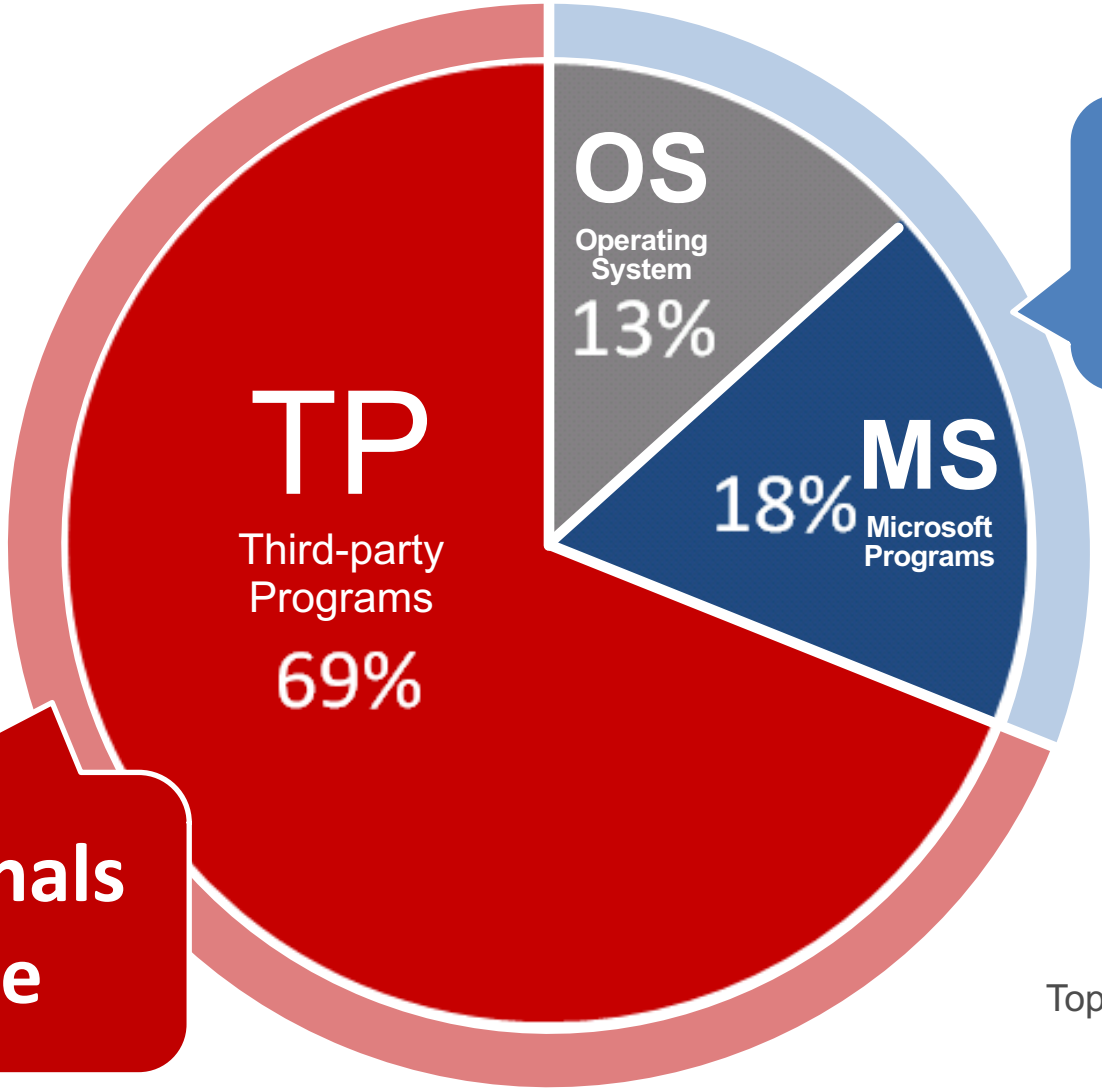
What are the major contributors of this increasing trend?

OS
Operating System

MS
Microsoft Programs

TP
Third-party Programs

Third-party programs are found to be almost exclusively responsible for this increasing trend



What you patch

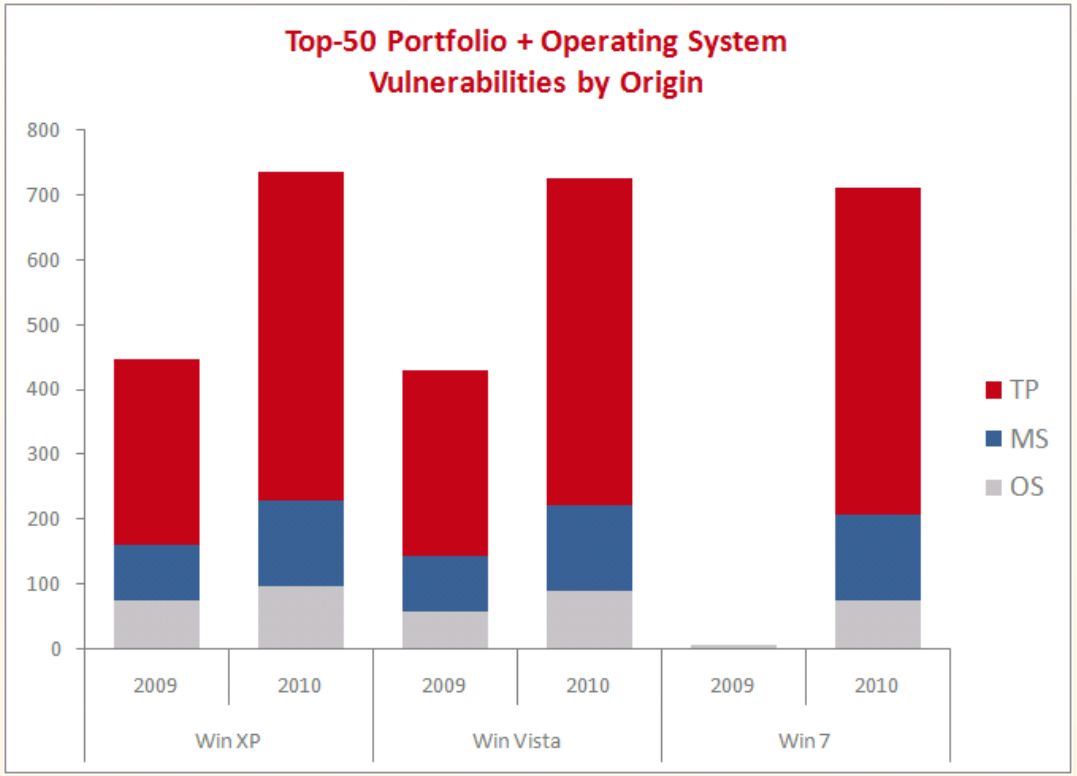
Cybercriminals don't care

Top-50 Portfolio & Windows XP Vulnerabilities in 2010

Third-party Programs Rule …

In 2010 an end-point with the Top-50 portfolio and Windows XP had:

- **3.83** times
  more vulnerabilities in the 24 third-party programs than in the 26 Microsoft programs
- **5.22** times
  more vulnerabilities in the 24 third-party programs than in the operating system



The Role of the Operating System

Top 50 Portfolio

2010

+

Advisories	163
Vulnerabilities	729

Advisories	153
Vulnerabilities	722

Vulnerabilities -1.0%

Advisories	148
Vulnerabilities	709

Vulnerabilities -2.7%

Updating a typical End-Point …

To keep a PC with the Top-50 portfolio fully patched, the user has to manage a total of

14 different update mechanisms

1

Update Mechanism

- to patch the OS and the 26 Microsoft programs,
- covering 31% of the vulnerabilities

13

Update Mechanisms

- to patch the 24 third-party programs,
- covering 69% of the vulnerabilities

Cybercriminals know

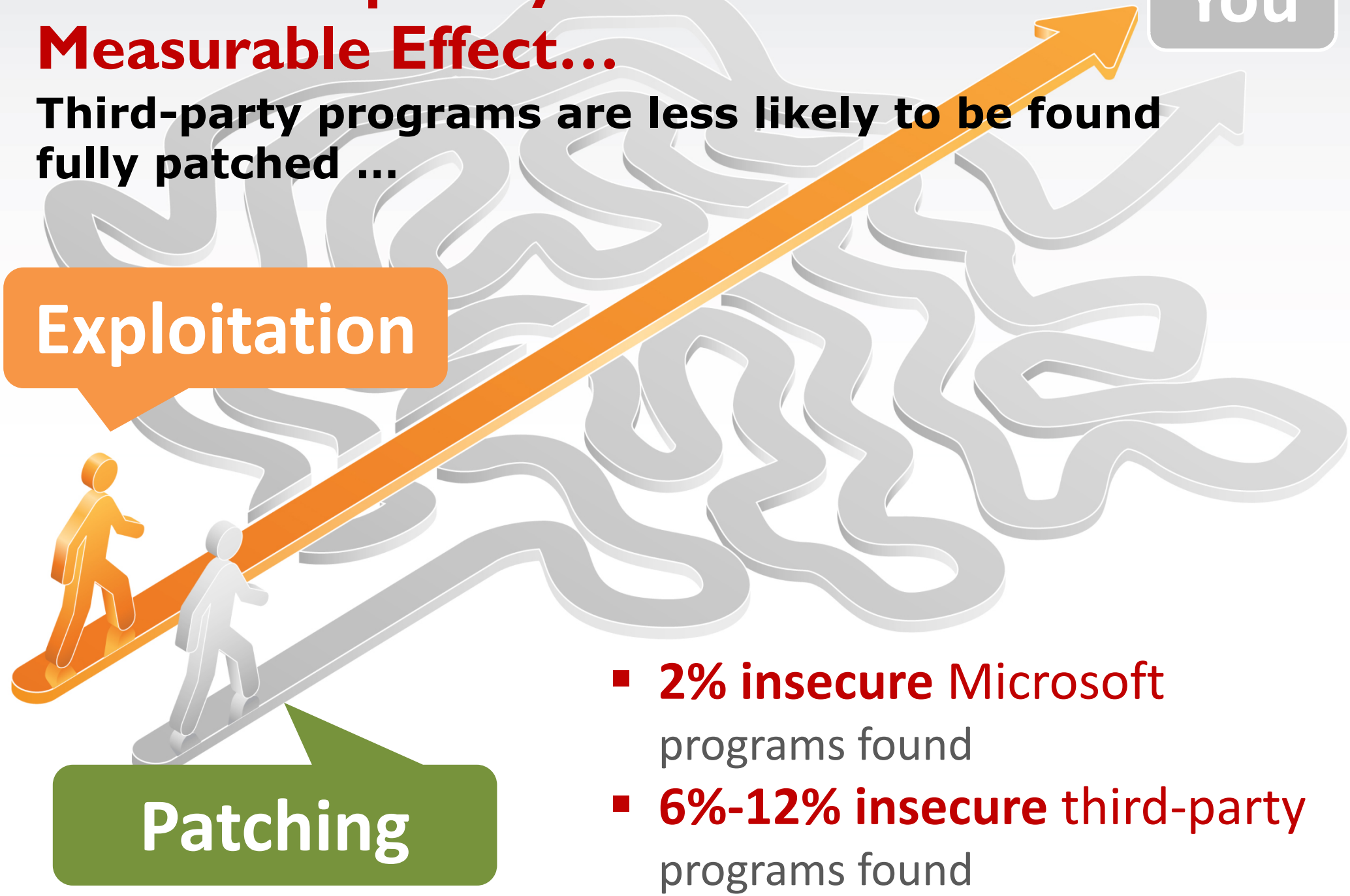
patch available

≠

patch installed

Patch Complexity has a Measurable Effect…

Third-party programs are less likely to be found fully patched …



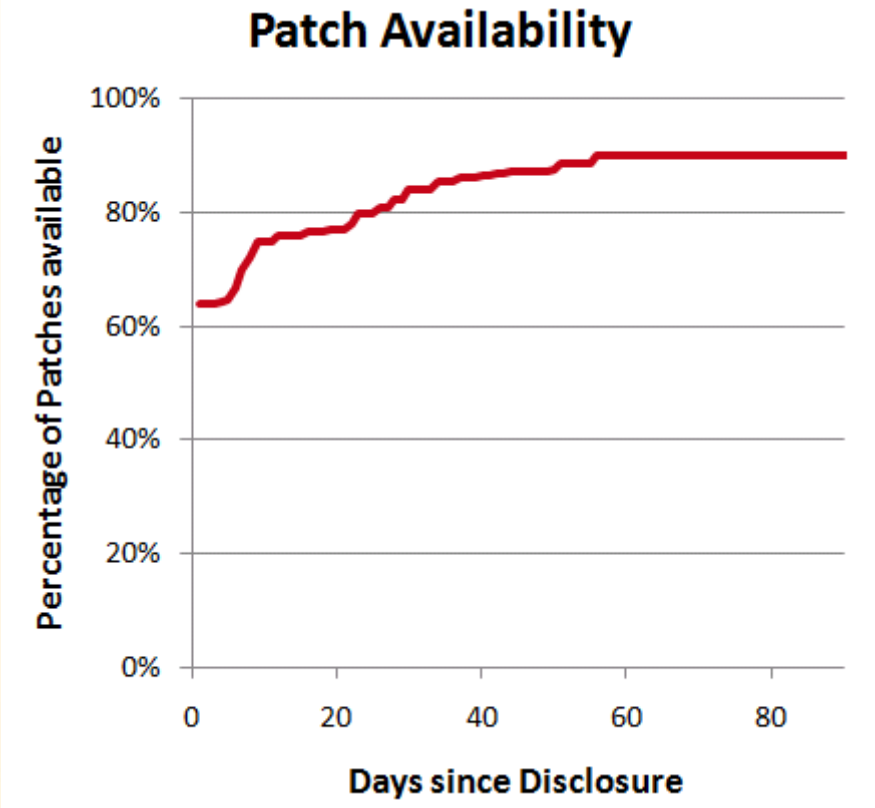
- **2% insecure** Microsoft programs found
- **6%-12% insecure** third-party programs found

Source: Secunia PSI scans 2010/Q4

However, Patches are Available!

Patch availability within N days upon vulnerability disclosure:

- 65% patch availability on the day of disclosure
- 75% patch availability within 10 days
- 90% patch availability within 56 days



Top-50 Portfolio & Windows XP

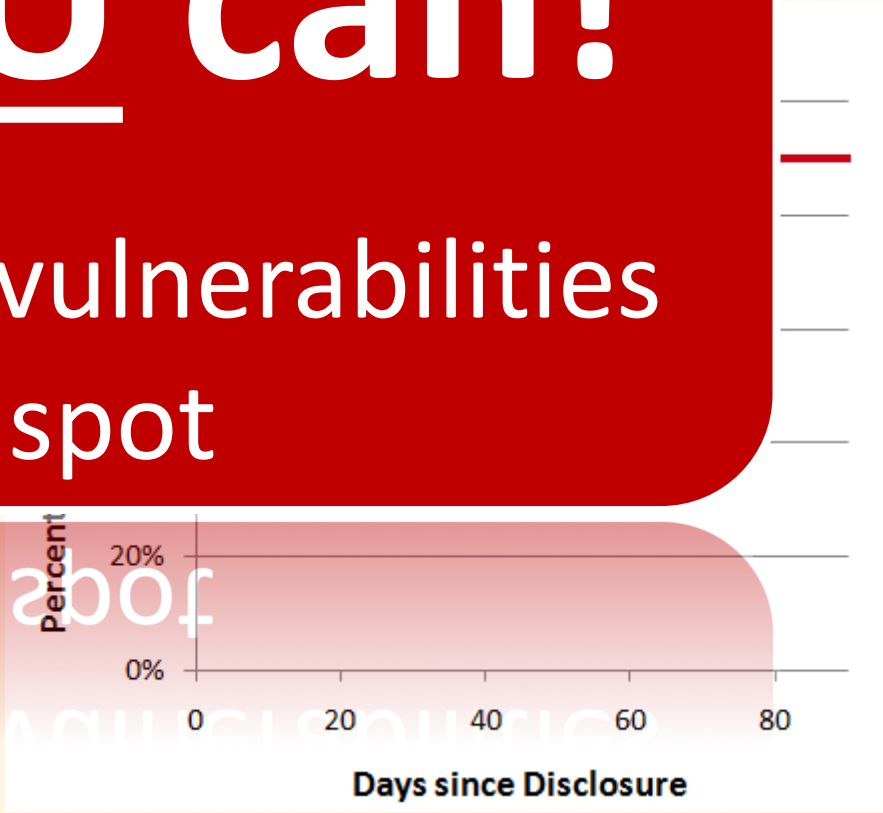
However, Patches are Available!

Patch availability within N days upon vulnerability disc

- 6
- 9
- 90% patch availability within 56 days

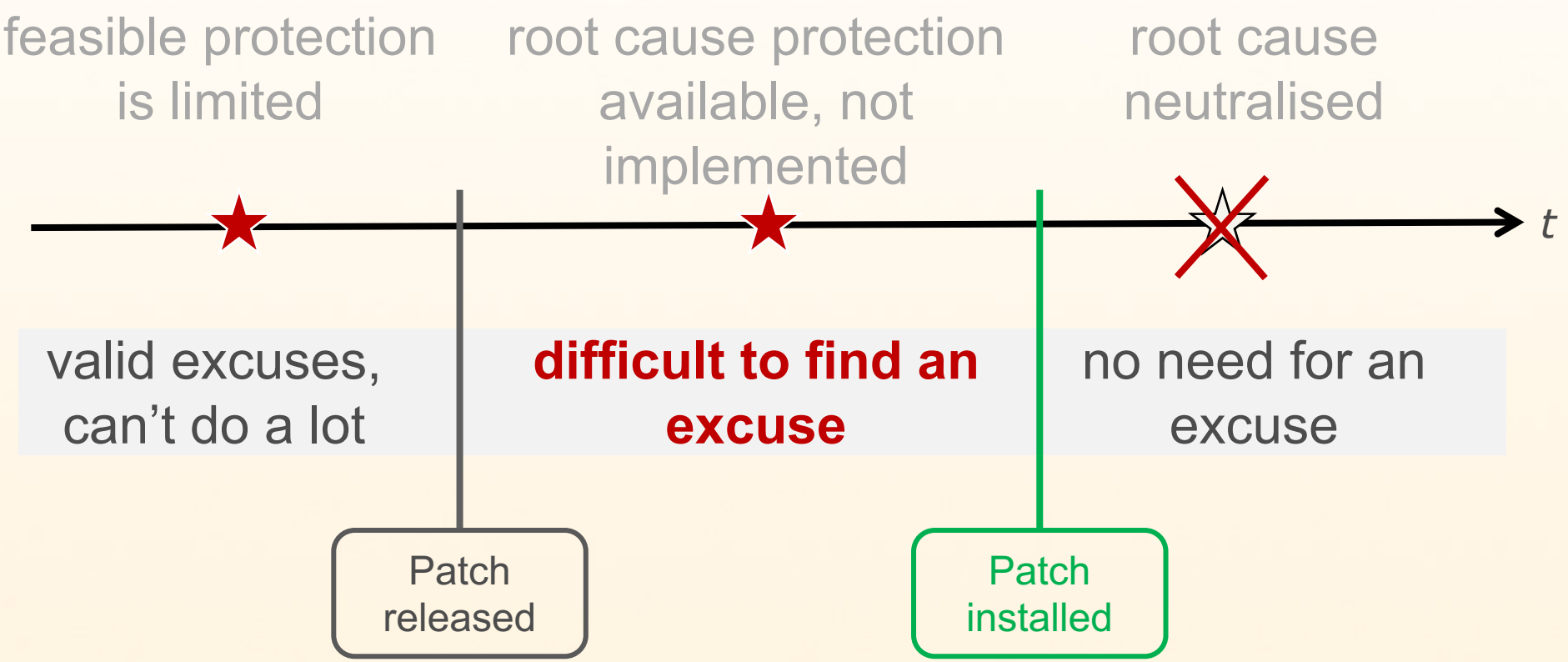
Yes YOU can!

.. fix 65% of the vulnerabilities on the spot



Responsibility

It is entirely your fault if you get infected after a patch is available



#Hosts x #Vulnerabilities
x {Complexity to stay secure}
=
Opportunity

A patch provides
better protection
than thousands of signatures

- it eliminates the
root cause

Patch Properties

A Patch…

- Has no false positives (no false alarms)
- Has no false negatives (no attacks that slip through the net)
- Introduces no latency or other delays
- Provides better protection than thousands of anti-virus signatures
- Consumes no resources whatsoever after deployment

Conclusion

- We still perceive the operating system and Microsoft products to be the primary attack vector, largely ignoring third-party programs
  - Just like locking the front door while the back door remains wide open
- Patching should be prioritised as a primary security measure given its effectiveness to neutralise attacks
- Controlled identification and timely patching of all programs, including third-party programs, is needed

Stay Secure!

Supporting Material

- Secunia Yearly Report 2010
  http://secunia.com/gfx/pdf/Secunia_Yearly_Report_2010.pdf
- RSA Paper "Security Exposure of Software Portfolios"
  http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf
- Secunia Personal Software Inspector (PSI)
  free for personal use http://secunia.com/psi
- Secunia Corporate Software Inspector (CSI)
  http://secunia.com/vulnerability_scanning/corporate
- Secunia Quarterly Security Factsheets
  http://secunia.com/factsheets