



# The Dynamics and Threats of End-Point Software Portfolios

Dr. Stefan Frei  
Research Analyst Director

Mail: [sfrei@secunia.com](mailto:sfrei@secunia.com)

Twitter: [@stefan\\_frei](https://twitter.com/stefan_frei)



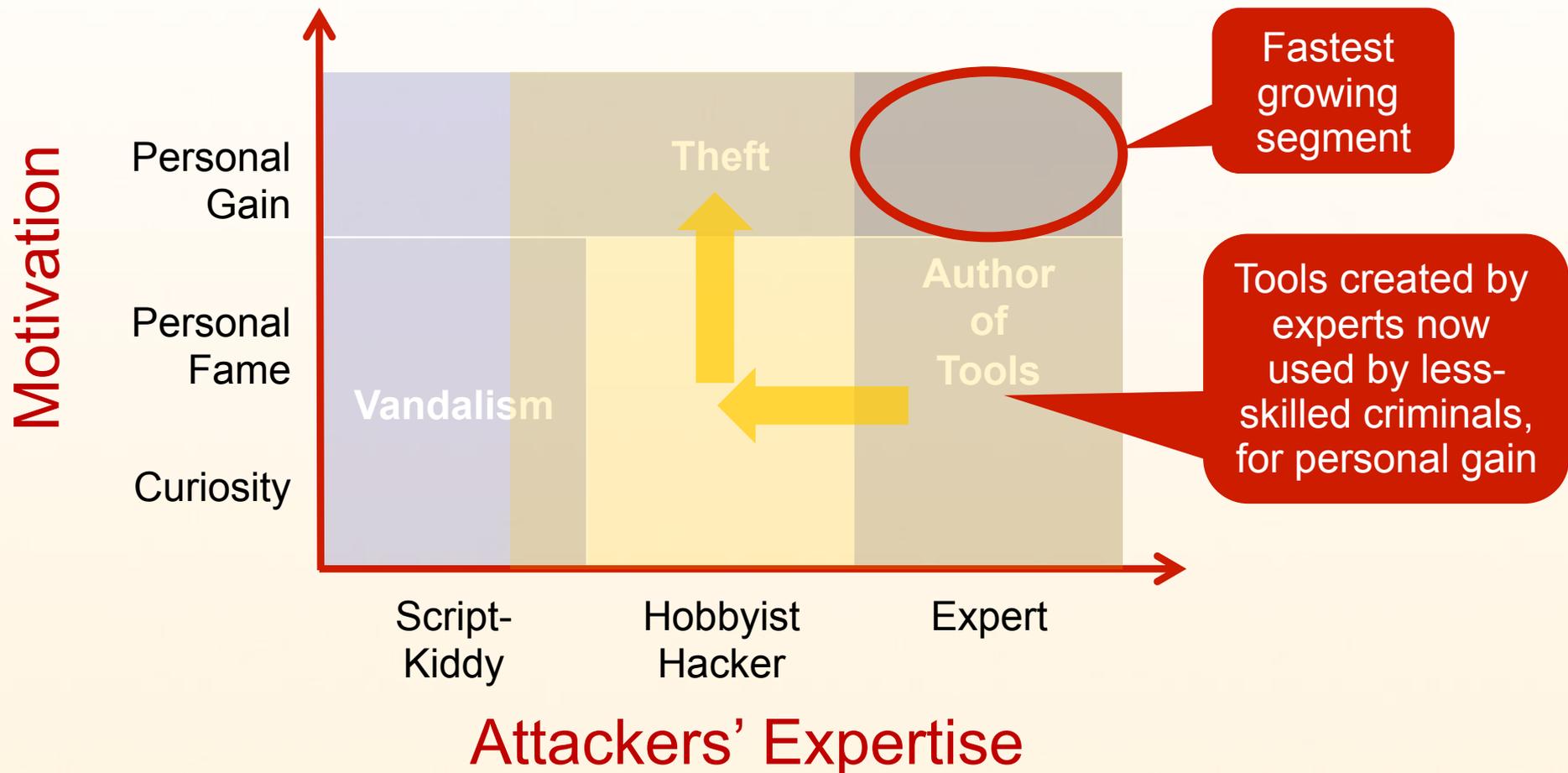
# Agenda

- The Changing Threat Environment
- Measuring the Complexity of End-Points
- Patch Adoption Dynamics



# The Changing Threat Environment

## Motivation vs. Expertise



# Malware as a Service (MaaS)



## Gold Edition

- 6 months (unlimited) or 9 months (maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messenger
- 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 changes 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

# Evolving Threats Summary

## 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

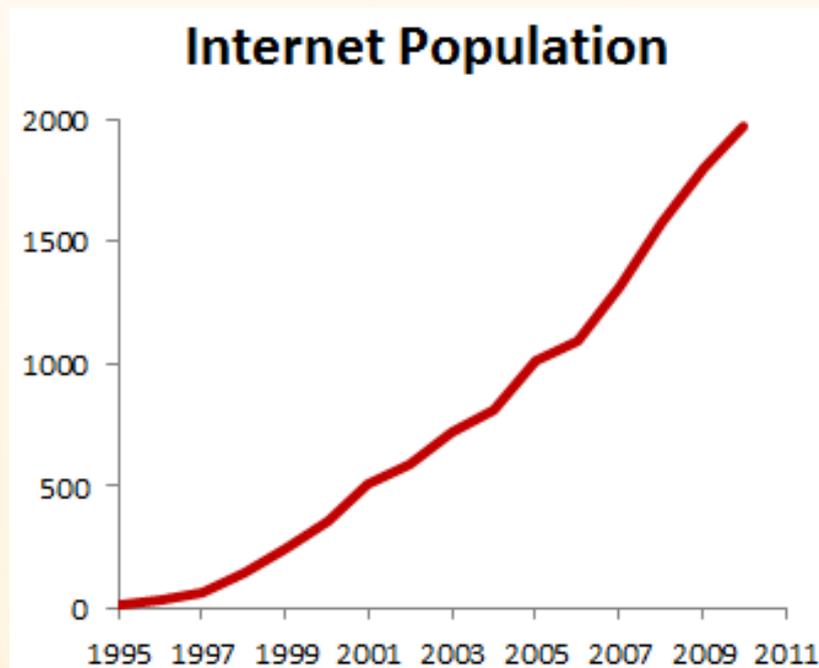
$$\#Hosts \times \#Vulnerabilities \\ = \\ Opportunity$$

# Worldwide Internet Usage



# 2,095 Million

estimated Internet users on March 31<sup>st</sup>, 2011



**31%** penetration of population

**448%** growth from 2000 to 2010

# 2,095 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

# From a Criminal's Perspective

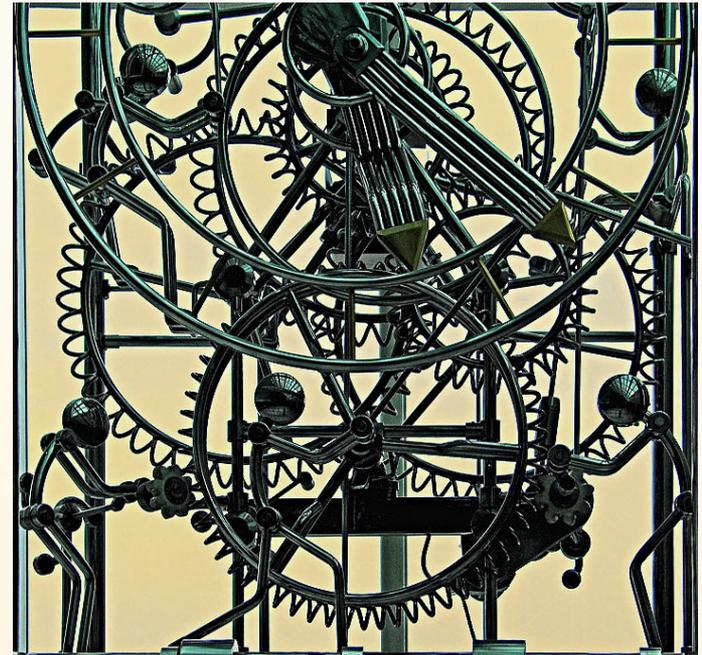
$$\#Hosts \times \#Vulnerabilities = Opportunity$$

# What does a typical End-Point look like?



## .. numerous **programs** and **plug-ins**!

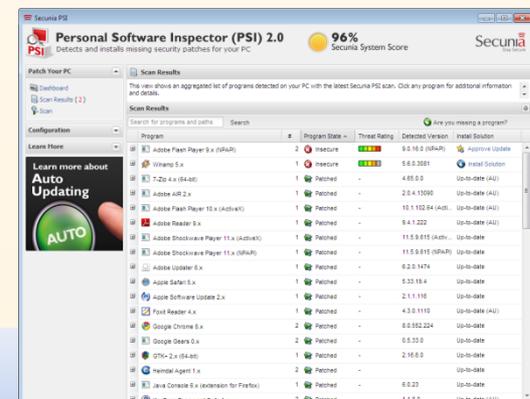
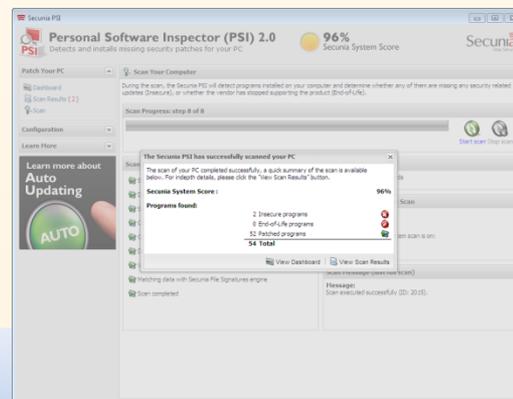
- **How many** programs do you think you have installed on your **typical** Windows machine?
- How many different **update mechanisms** do you need to keep this PC up-to-date?





# Data from Real End-Points in the Field

- Scan results from more than 4.0 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

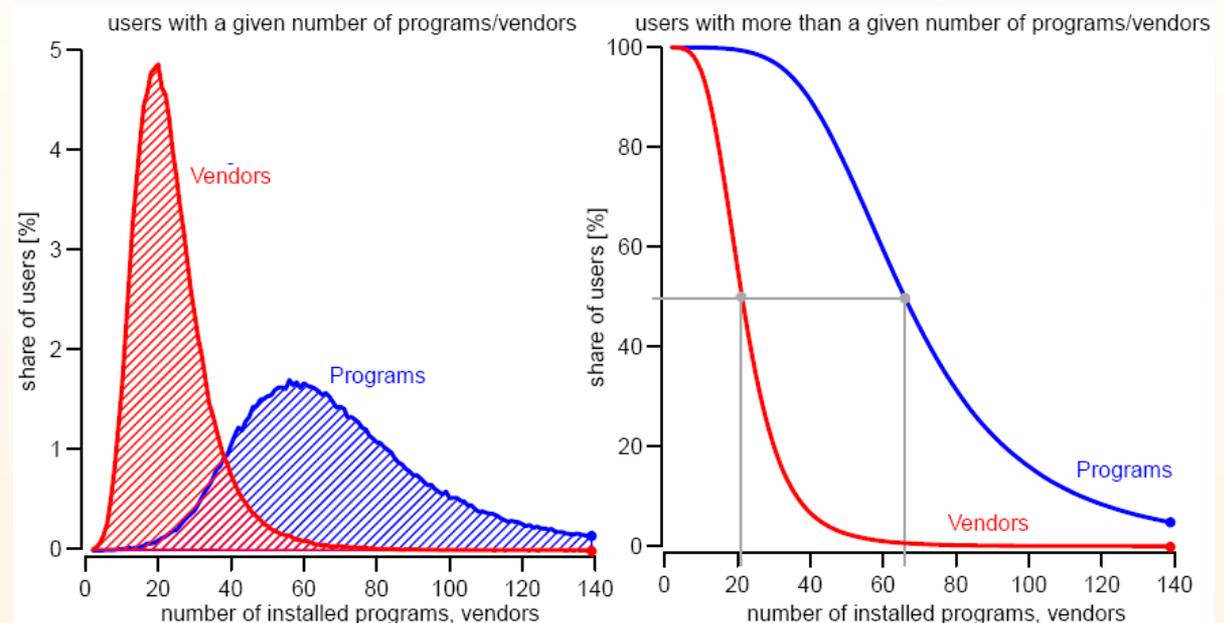


# Software Portfolios ...

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



# The Top-50 Software Portfolio

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

**14**

Vendors

**26**

Microsoft

**24**

Third-  
party

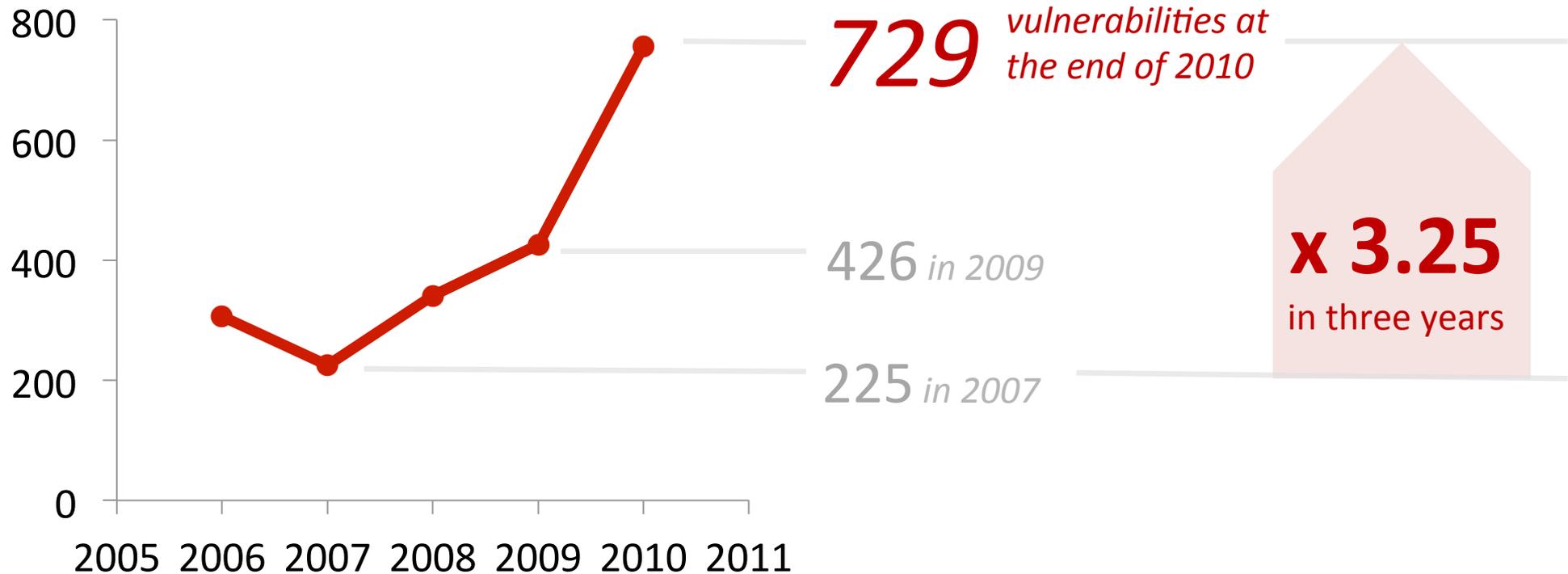
**26 Microsoft and 24 third-party (non-Microsoft) programs  
from 14 different vendors**

# An Alarming Trend ...



Vulnerabilities affecting a typical end-point increased **71%** from 2009 to 2010 alone

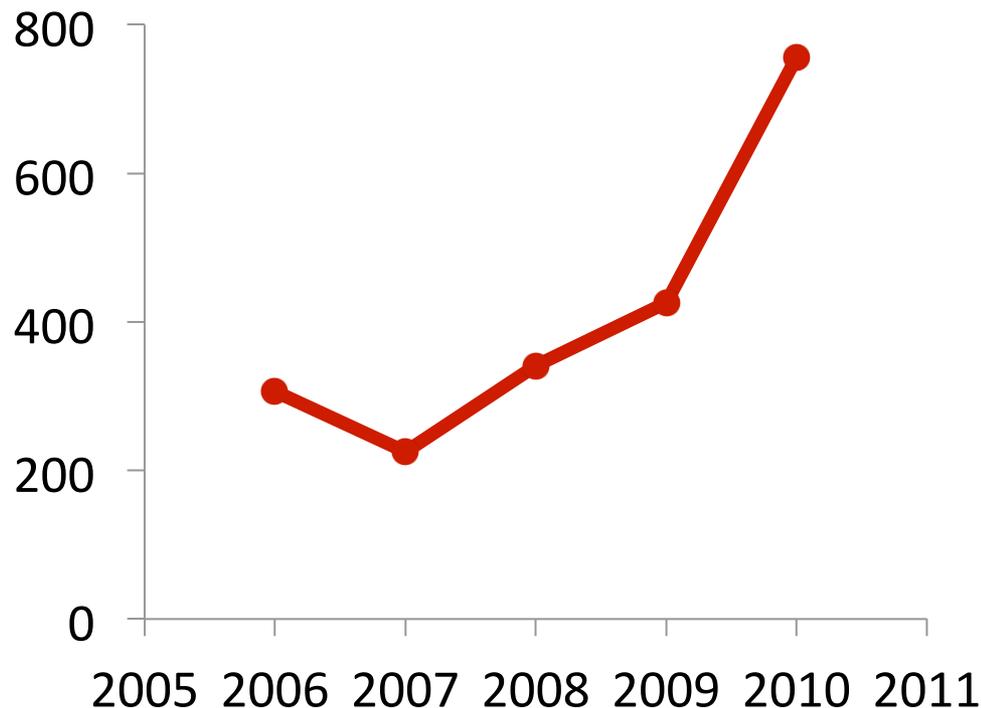
Top-50 Portfolio with Windows XP  
Vulnerabilities



# A Relevant Trend ...



Top-50 Portfolio with Windows XP Vulnerabilities



**>70%** of these vulnerabilities are rated as **Highly** or **Extremely critical**

**>90%** of these vulnerabilities are **exploitable from remote**

**>50%** of these vulnerabilities **provide system access to the attacker**

# What is the source of this increasing trend?



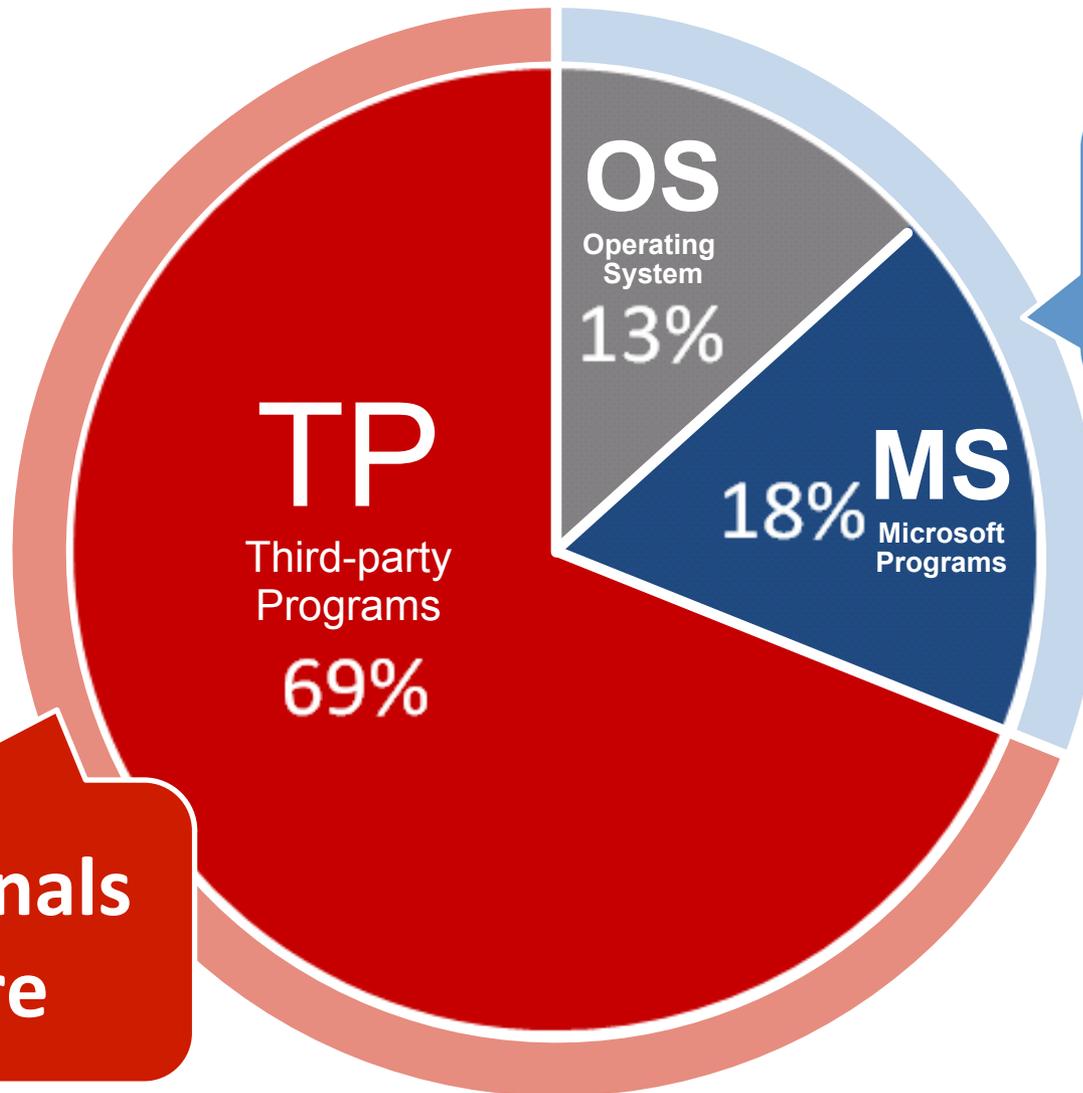
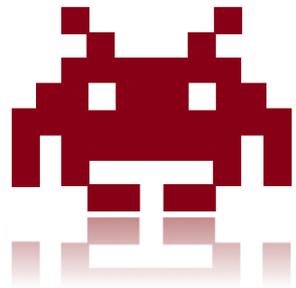
**OS**  
Operating  
System

**MS**  
Microsoft  
Programs

**TP**  
Third-party  
Programs

# Third-party programs

are found to be almost exclusively responsible for this increasing trend



What you patch

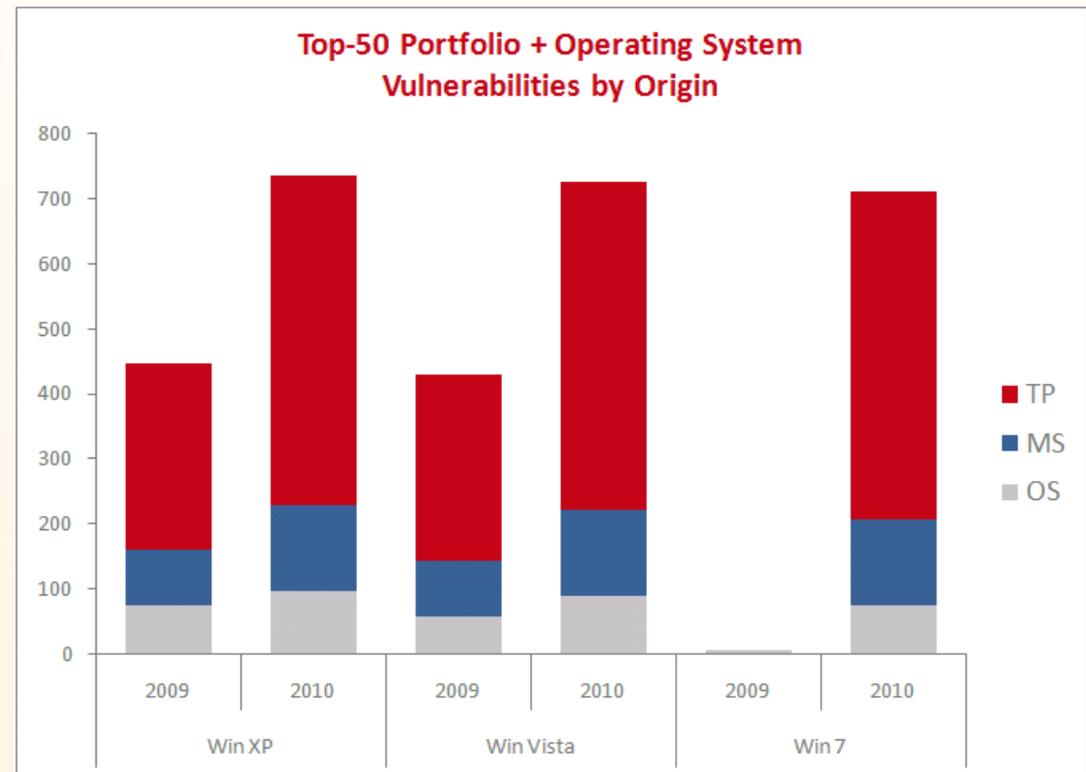
Cybercriminals don't care



## Third-party Programs Rule ...

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

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



# The Role of the Operating System



Top 50 Portfolio  
2010

+



Microsoft  
**Windows** xp

Advisories	163
Vulnerabilities	729



Windows Vista™

Advisories	153
Vulnerabilities	722



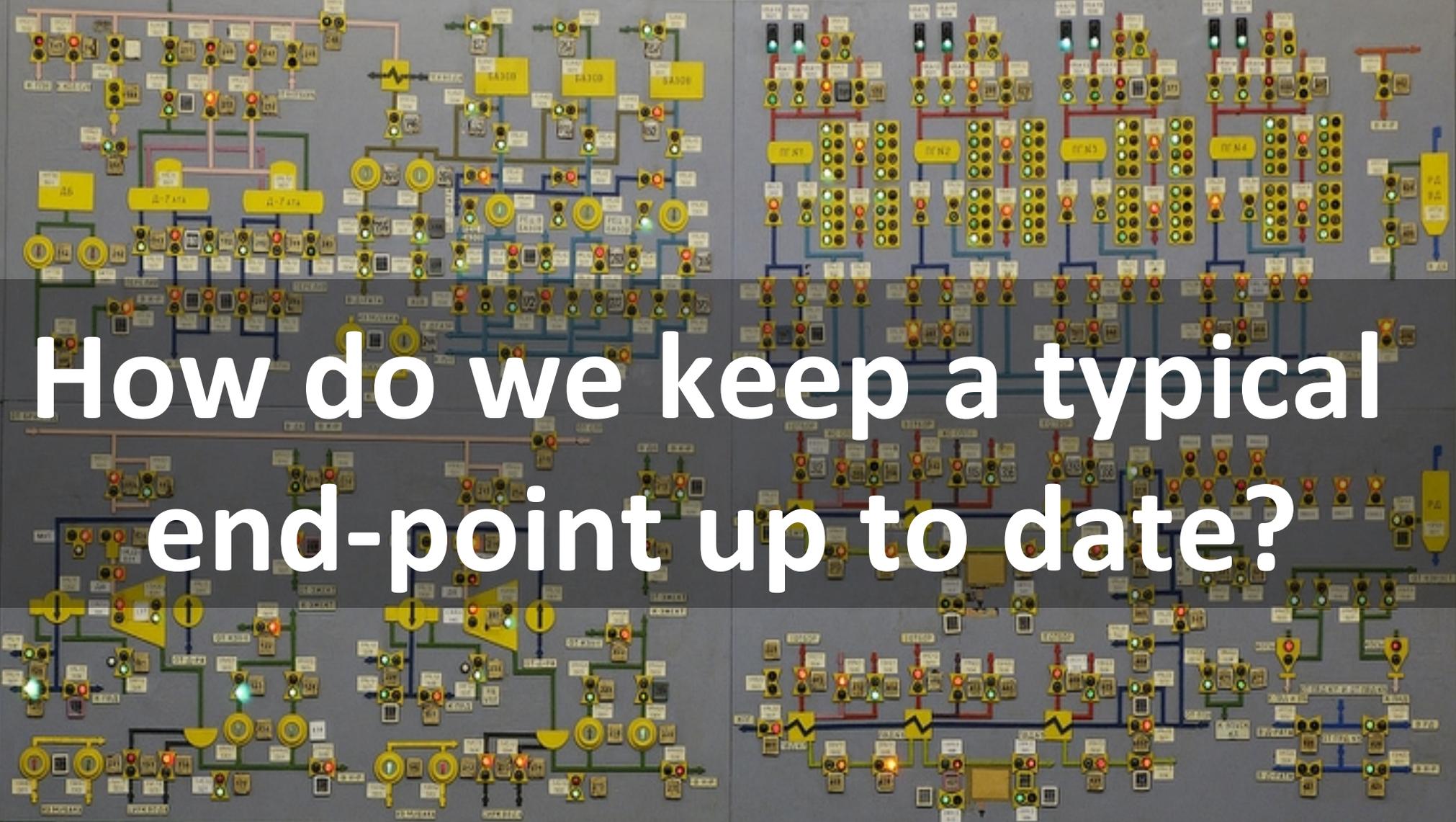
Windows 7

Advisories	148
Vulnerabilities	709

Vulnerabilities -1.0%

Vulnerabilities -2.7%

# How do we keep a typical end-point up to date?

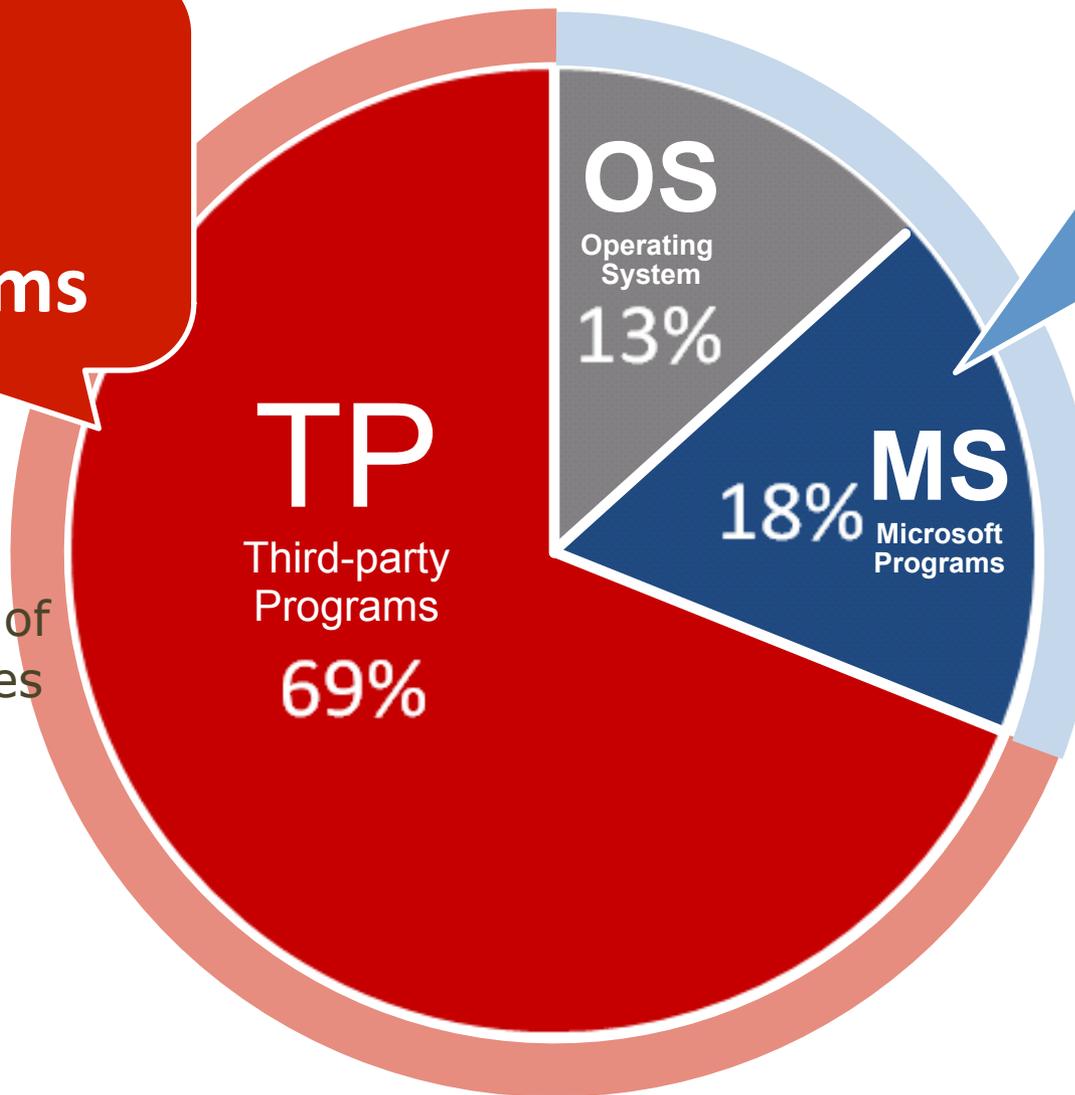


# 14 different update mechanisms

.. are needed to keeping a typical end-point up to date

**13**  
update  
mechanisms

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



**1**  
update  
mechanism

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

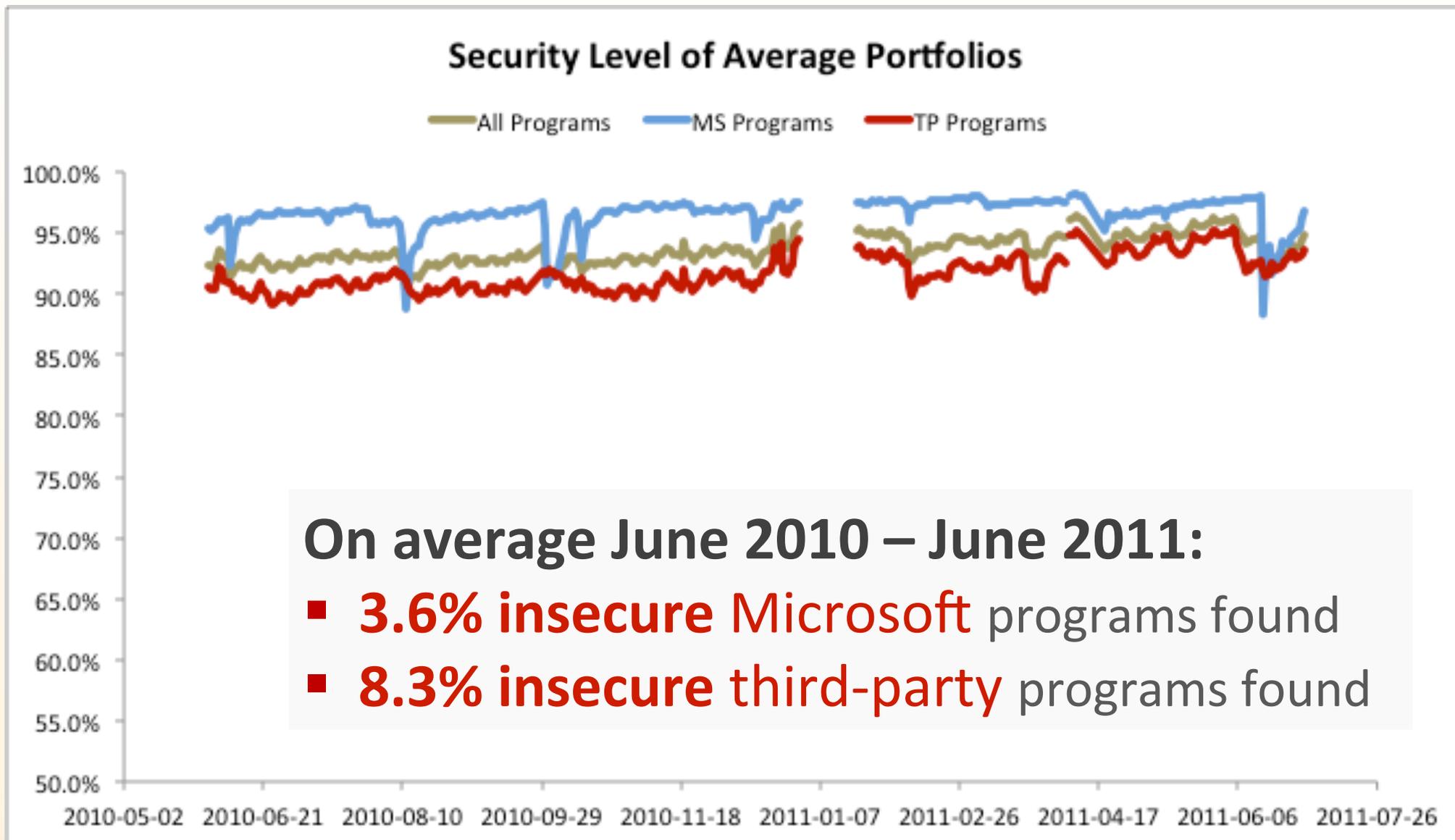
# Cybercriminals know

patch available

≠

patch installed

# Patch Complexity has a measurable effect...





**Are we doomed?**

# Patches are Available!

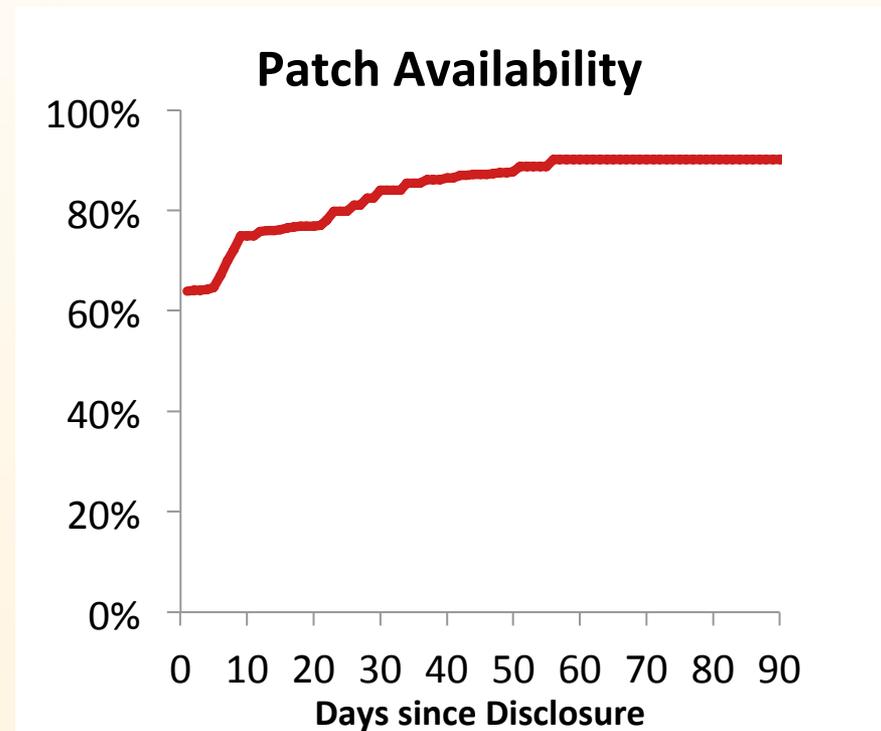


Availability of security patches within N days upon vulnerability disclosure:

**65%** patch availability on the day of **disclosure**

**75%** available within **10 days**

**90%** available within **56 days**



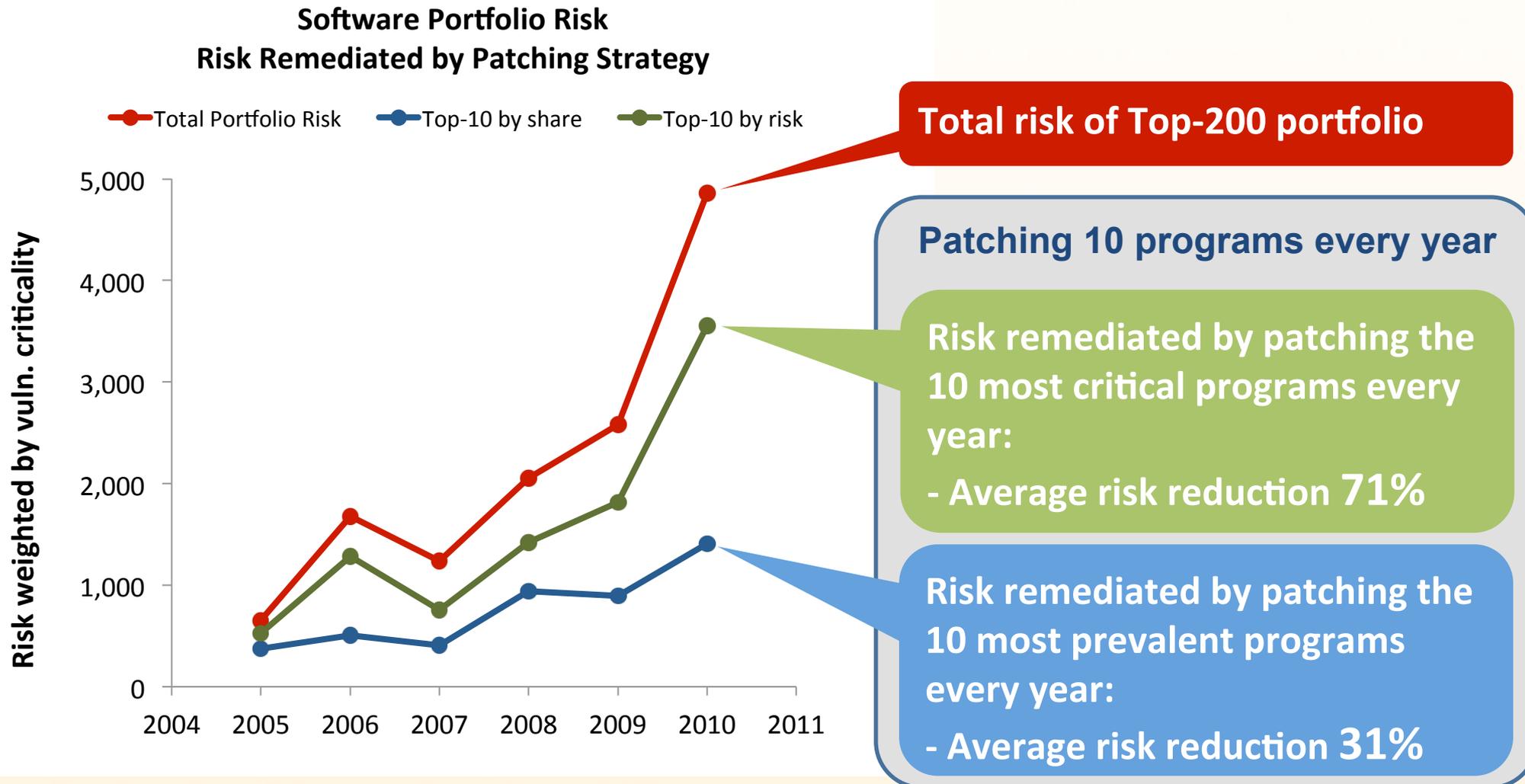
# What if you can't patch all programs?

Lets take the 200 most prevalent programs found in the field

- You have the resources to patch 10 of the 200 programs
- Let's analyze two strategies of selecting the 10 programs

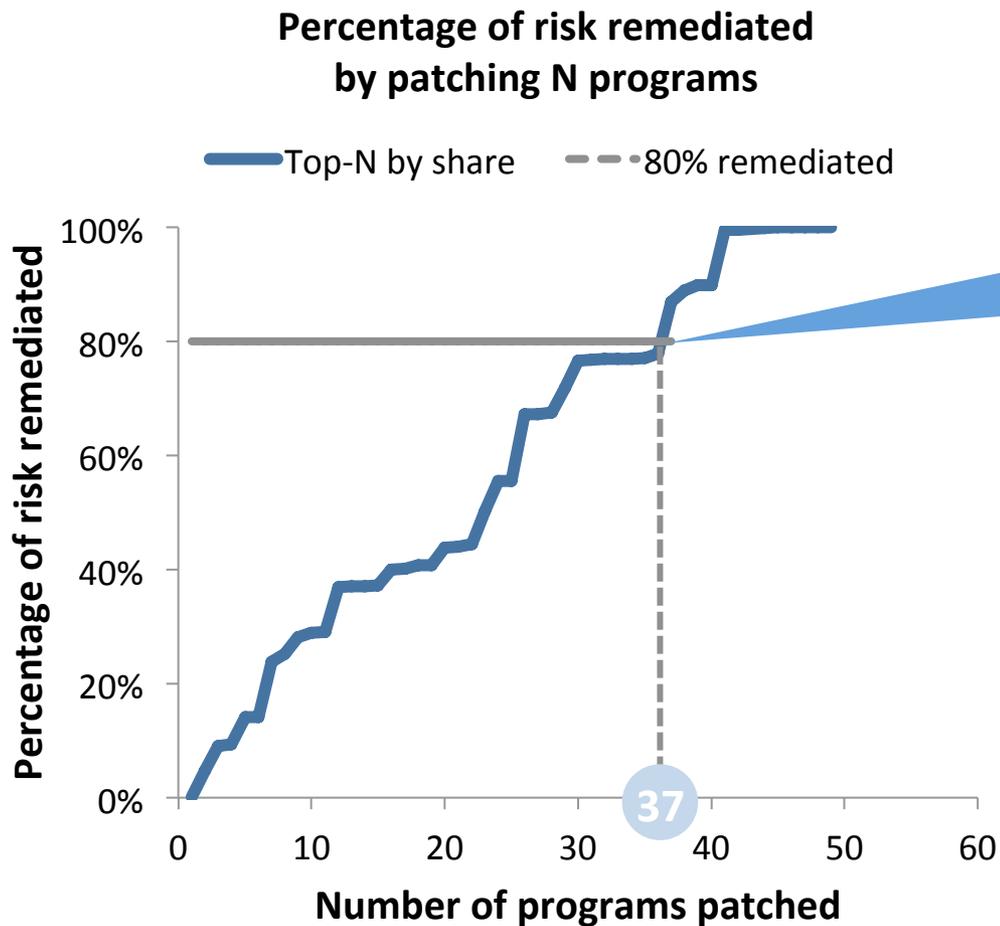
# Patch Strategies

## Patching 10 of 200 programs with different strategies



# Patch Strategies

## Statically patching the most prevalent programs



Patching  $N$  of 200 programs

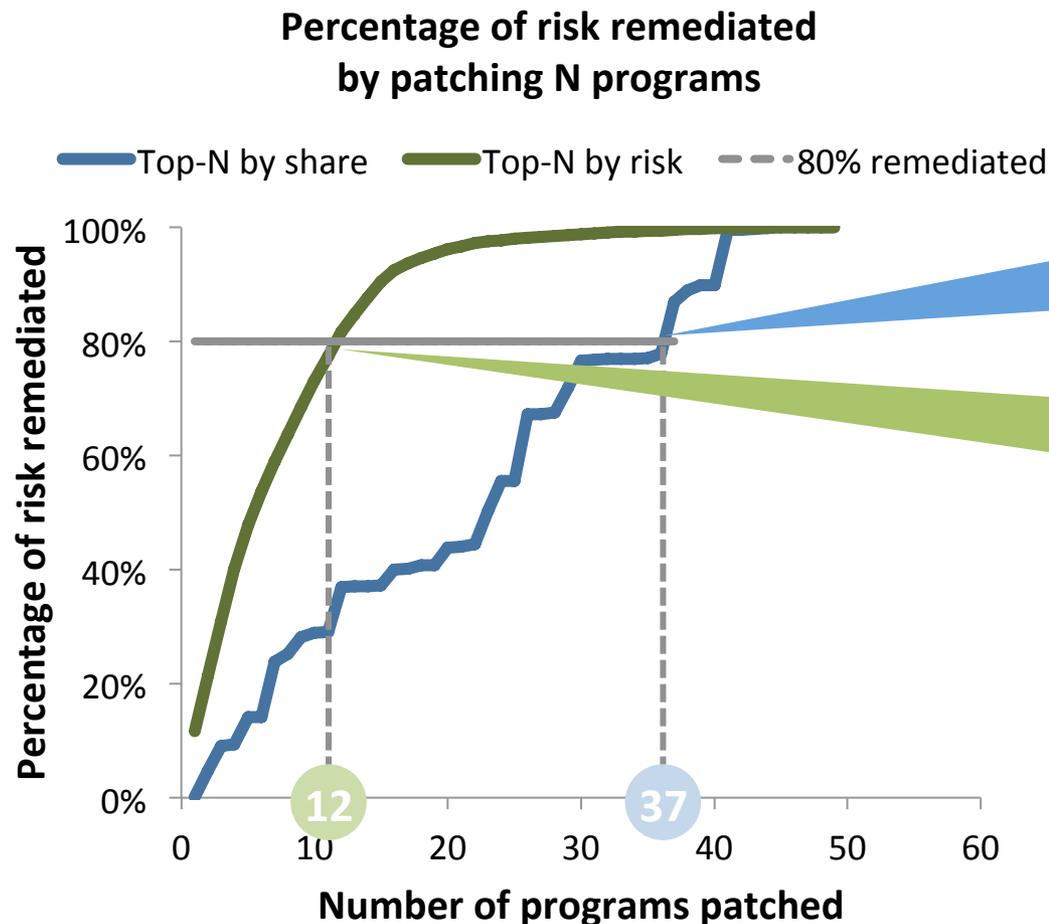
**Strategy 1: Static**

Risk remediated by patching the  $N$  most prevalent programs

80% risk reduction achieved by patching the **37 most prevalent** programs

# Achieve more with less

Knowing what to patch pays out!



Patching N of 200 programs

**Strategy 1: Static**

Risk remediated by patching the N most prevalent programs

**Strategy 2: By Criticality**

Risk remediated by patching the N most critical programs

80% risk reduction achieved by either patching the **12 most critical** programs, or by patching the **37 most prevalent** programs

$$\begin{aligned} & \# \text{Hosts} \times \# \text{Vulnerabilities} \\ & \times \{ \text{Complexity to stay secure} \} \\ & = \\ & \text{Opportunity} \end{aligned}$$

# Conclusion

## Lock the right doors

- 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
- 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](http://secunia.com/gfx/pdf/Secunia_Yearly_Report_2010.pdf)
- RSA Paper "Security Exposure of Software Portfolios"  
<http://bit.ly/eQbwus>
- How to Secure a Moving Target with Limited Resources  
<http://bit.ly/hzzlPi>
- Secunia Quarterly Security Factsheets  
<http://secunia.com/factsheets>
- Secunia Personal Software Inspector (PSI)  
free for personal use  
<http://secunia.com/psi>