Secunia
Stay Secure

The Dynamics and Threats of End-Point Software Portfolios

Dr. Stefan Frei
Research Analyst Director

Mail: sfrei@secunia.com
Twitter: @stefan_frei

Agenda

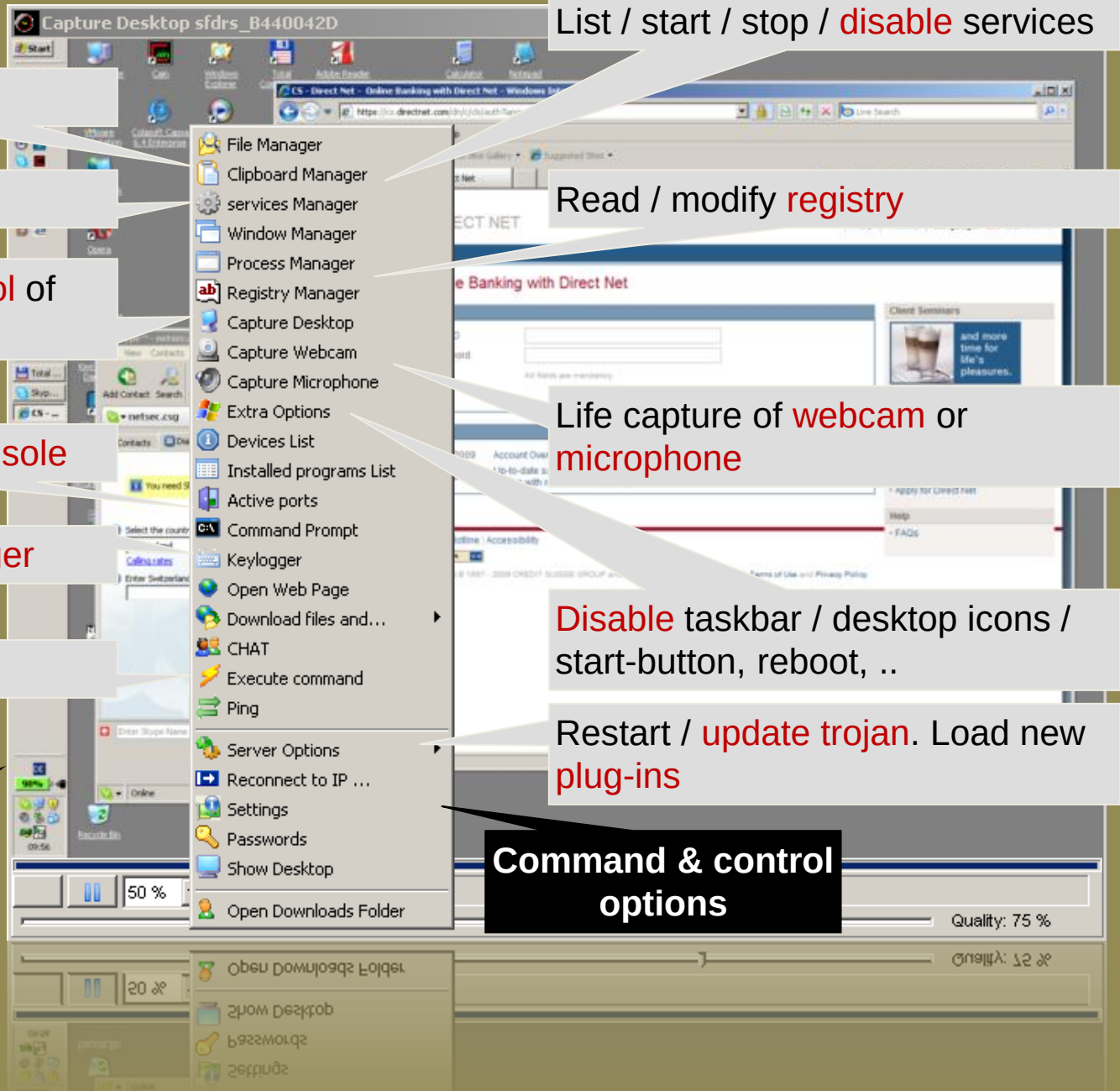
- The Changing Threat Environment
- Demo with Malware Construction Kit
- Measuring the Complexity of End-Points
  (or the Easy Prey for Cyber Criminals)
- Protective Measures when the Perimeter Failed

Malware Construction Kit
Live Demonstration

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

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, ..

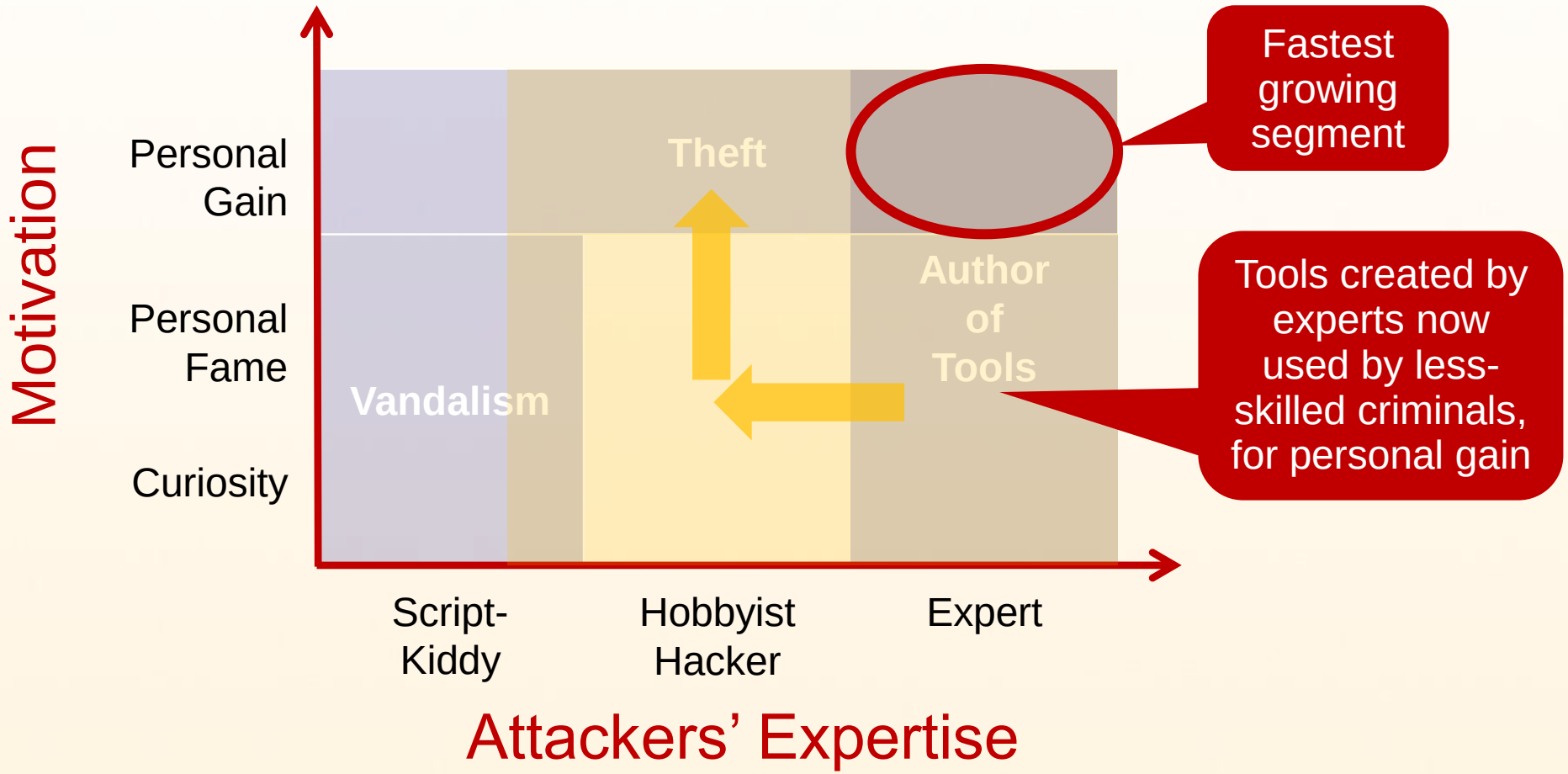
Restart / update trojan. Load new plug-ins

Life remote target session

Command & control options

The Changing Threat Environment

Motivation vs. Expertise



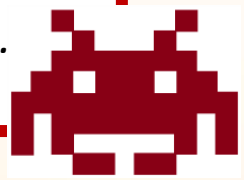
Source: Microsoft

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

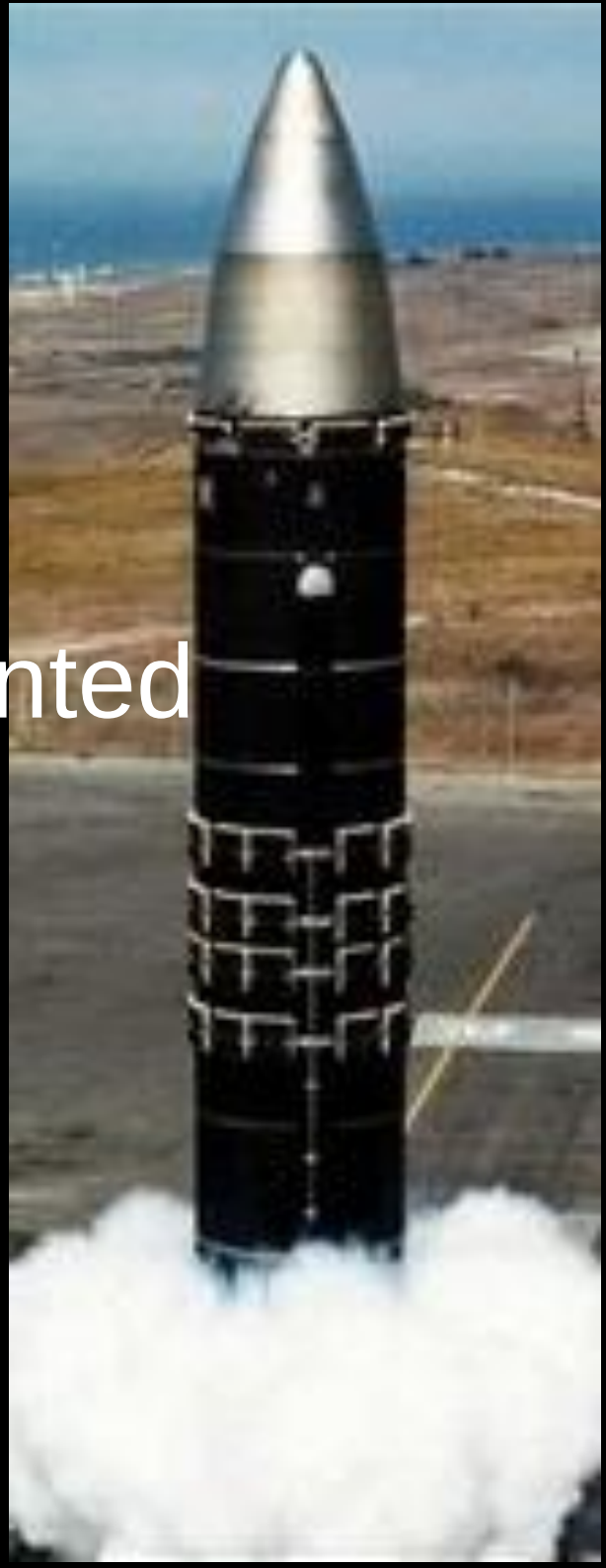

Malware D
Obfusca
1
Origin
Creat
func
DD
s
2
Per
Obfusca
Create mu
variants to
detection eng
ent
are that
QA (not
is used for
ent
Only
variants that pass
quality assurance
(bypass antivirus)
are used for
attacks!
Image: www.swisscyberstorm.com
Source: Damballa http://bit.ly/SerVar

An Arms Race …

286 million

virus samples counted in 2010

783,562	samples / day
32,648	samples / hour
544	samples / minute
9	samples / second



Source: Symantec Internet Security Threat Report (ISTR), Volume 16

Limitations of Traditional Protection

NSS Labs test of 2010/Q3:

25% of 123 publicly known exploits missed by top 10 prevention software

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

Up to 9% of the end-points in enterprises are found to be bot infected

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

Malware as a Service (MaaS)

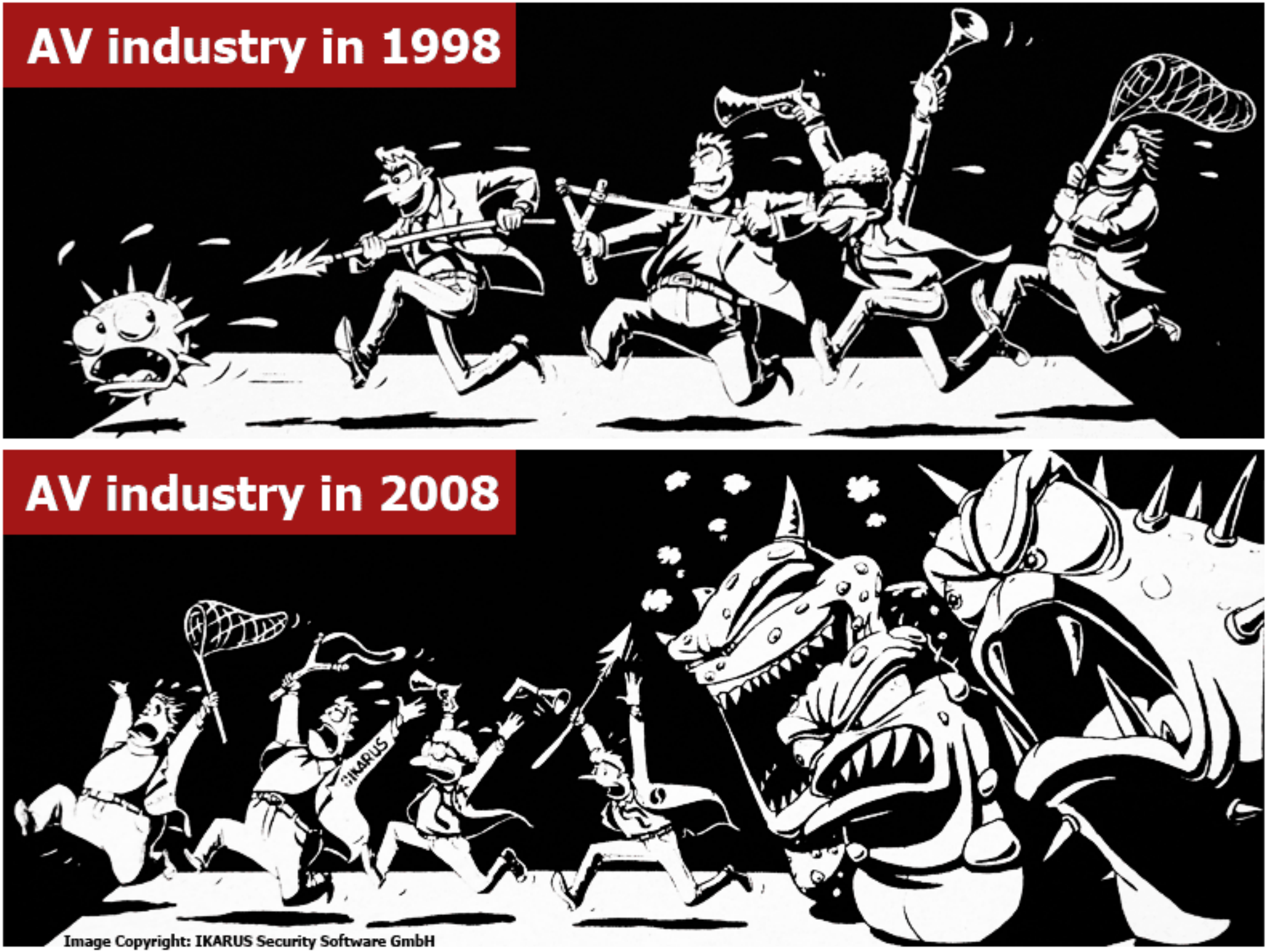
Gold Edition

- 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

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 x #Vulnerabilities

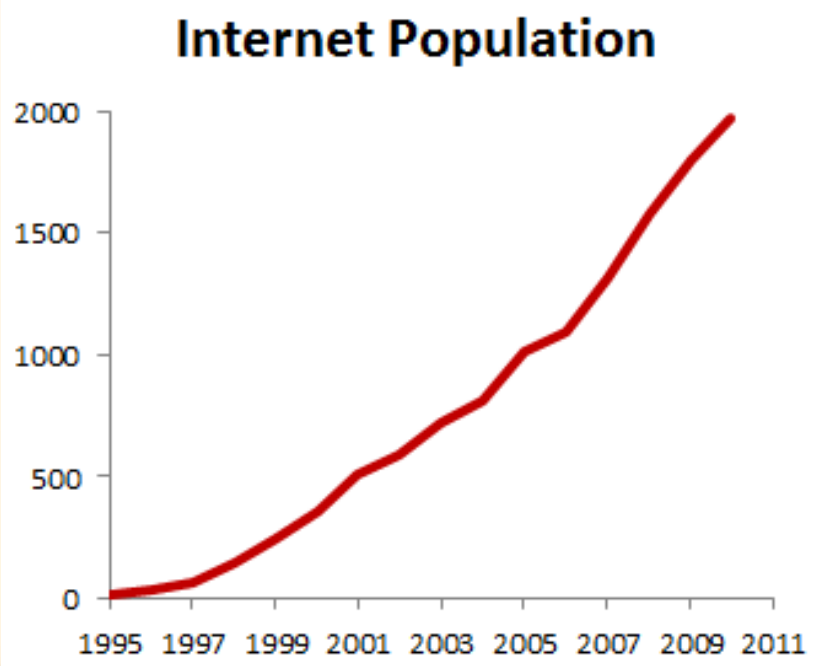
=

Opportunity

Worldwide Internet Usage

2,095 Million

estimated Internet users on March 31st, 2011



31% penetration of population

448% growth from 2000 to 2010

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

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 x #Vulnerabilities

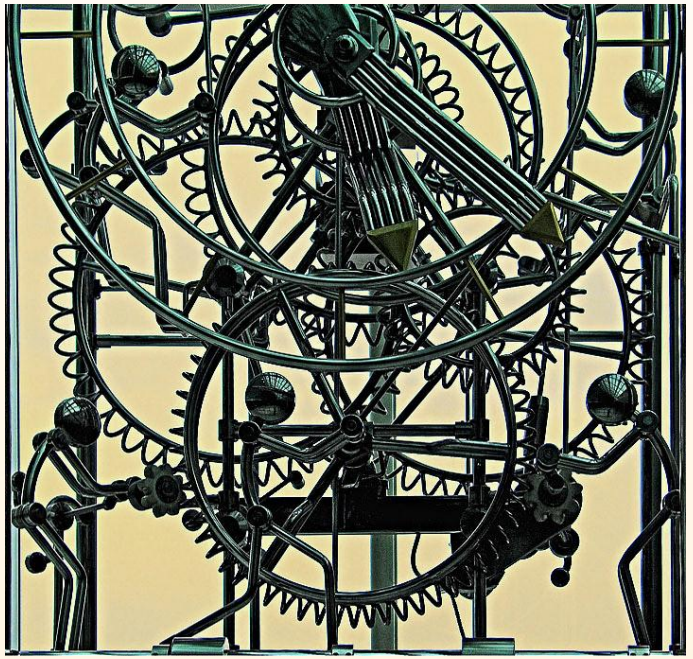
=

Opportunity

What does a typical End-Point look like?

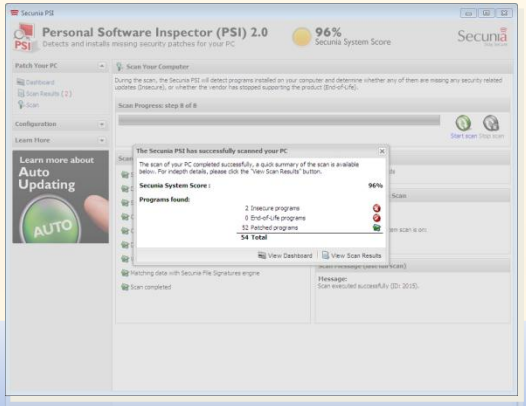
.. numerous programs and plug-ins!

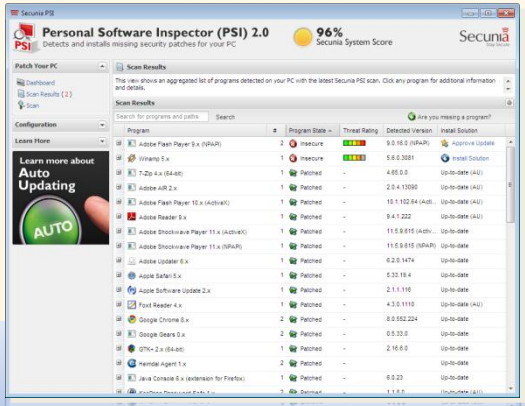
- How many programs do you think you have installed on your typical Windows machine?
- How many different update mechanisms do you need to keep this PC up-to-date?



Data from Real End-Points in the Field

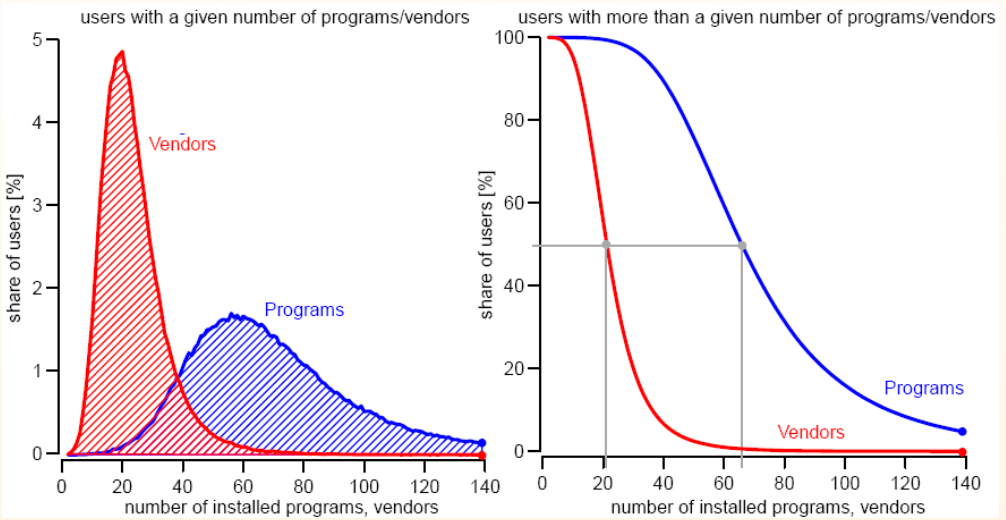
- Scan results from more than 3 Mio PSI users
  - Secunia Personal Software Inspector (PSI)
  - Free for personal use http://secunia.com/psi
- A lightweight software inspector/scanner to:
  - Identify insecure programs and plug-ins
  - Automatically install missing patches





Software Portfolios ...

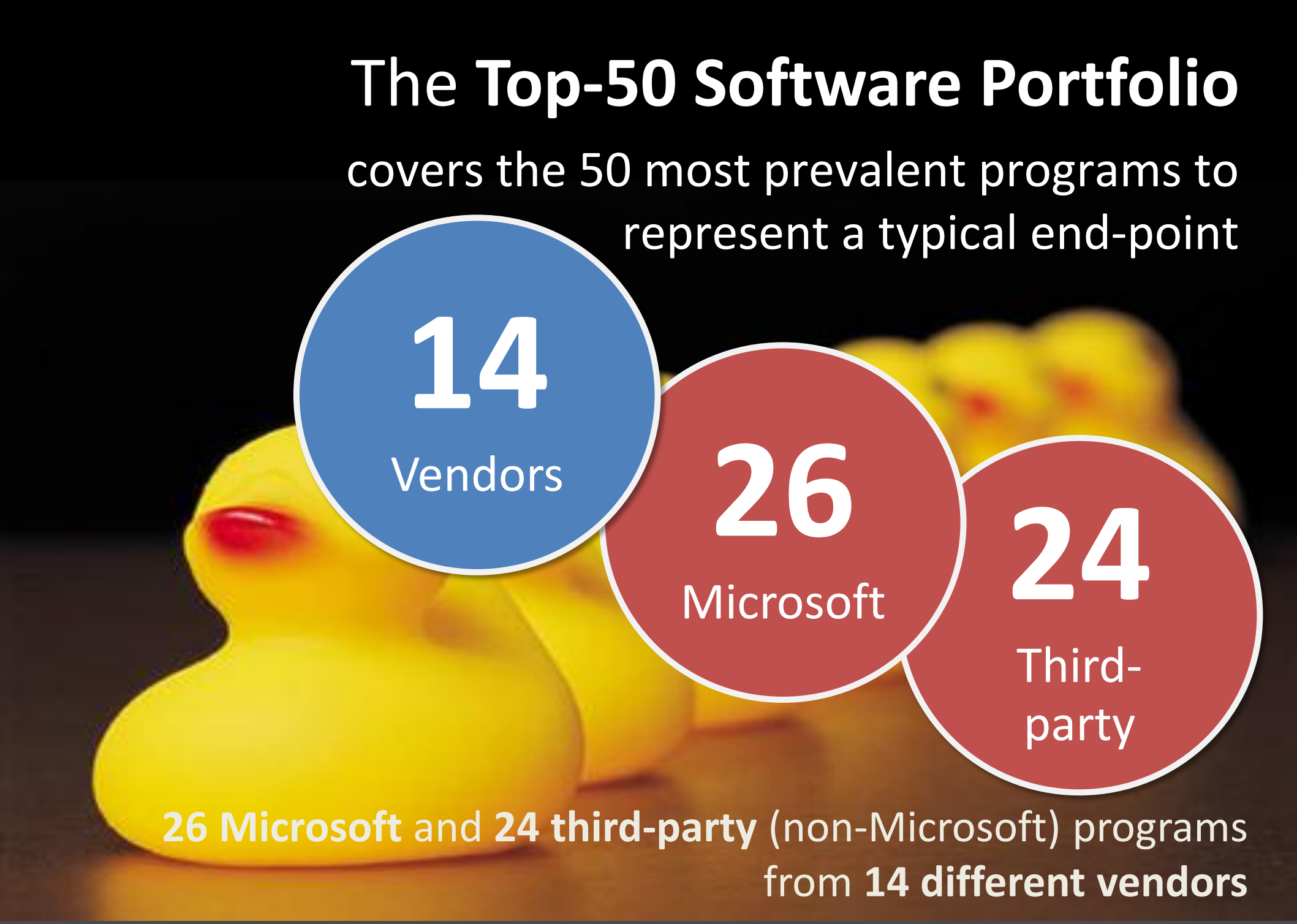
What programs do users typically have installed on their end-point PCs?



50% of users

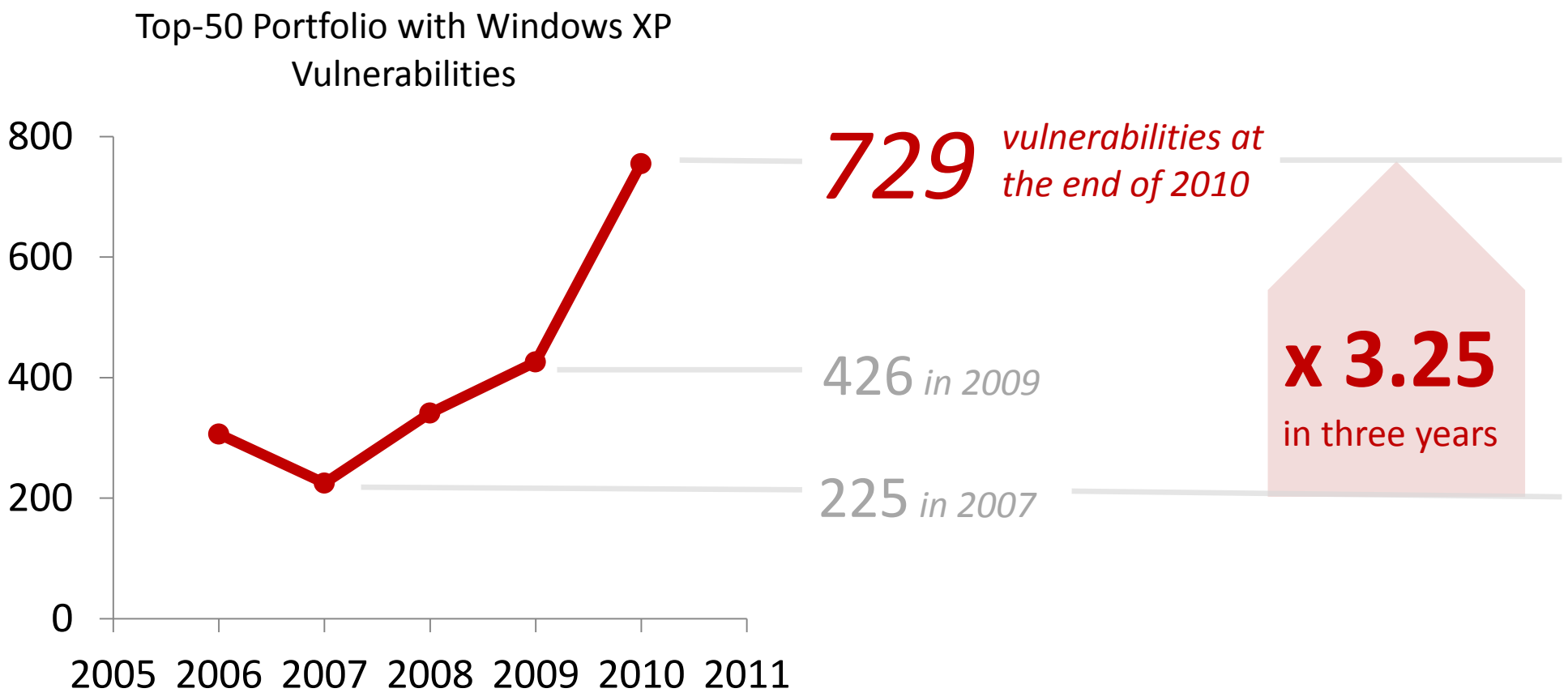
- have more than **66 programs**
- from more than **22 vendors** installed

Analysis based on Secunia PSI scans in 2010

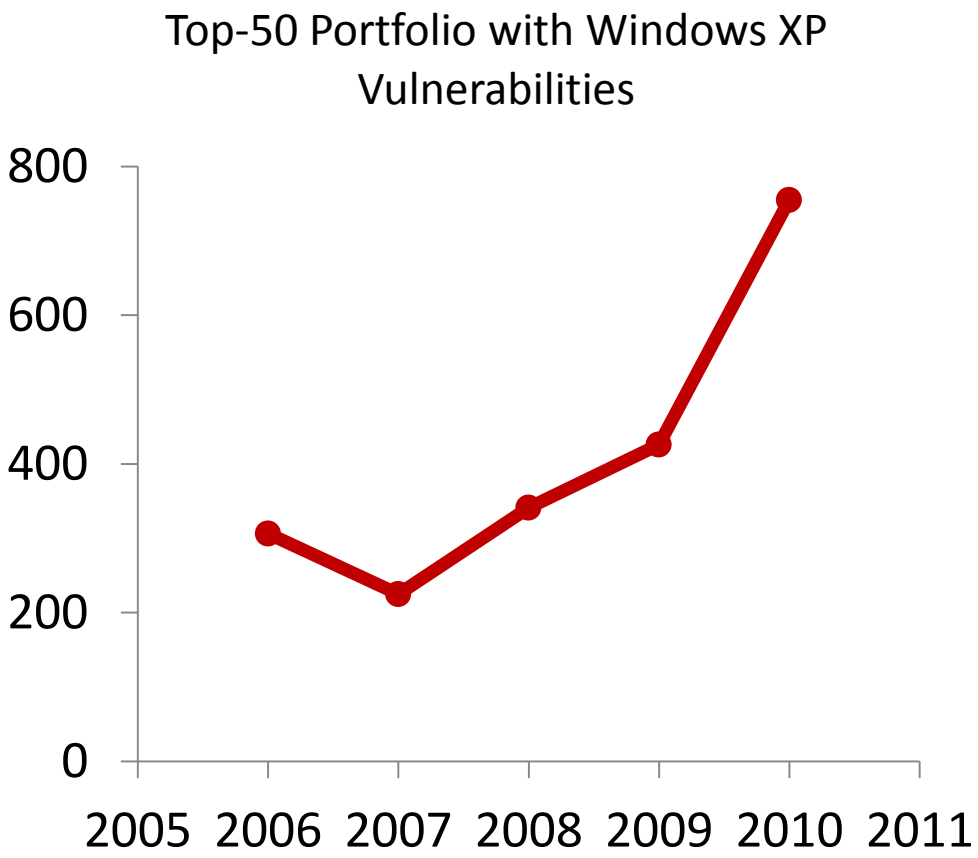

The **Top-50 Software Portfolio**
covers the 50 most prevalent programs to represent a typical end-point
14
Vendors
26
Microsoft
24
Third-party
26 Microsoft and **24 third-party** (non-Microsoft) programs
from **14 different vendors**

An Alarming Trend …

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



A Relevant Trend …



>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

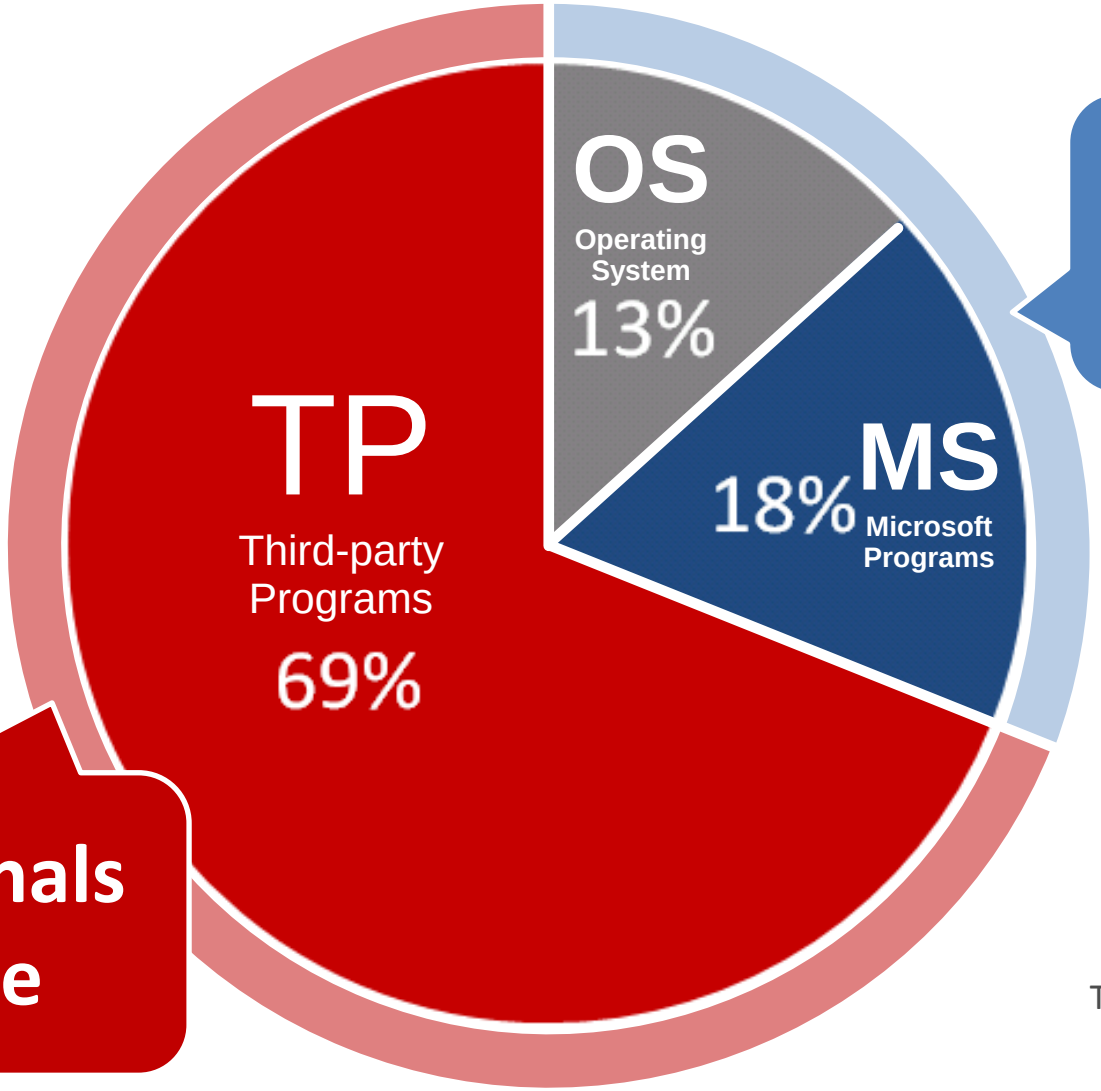
What is the source of this increasing trend?

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

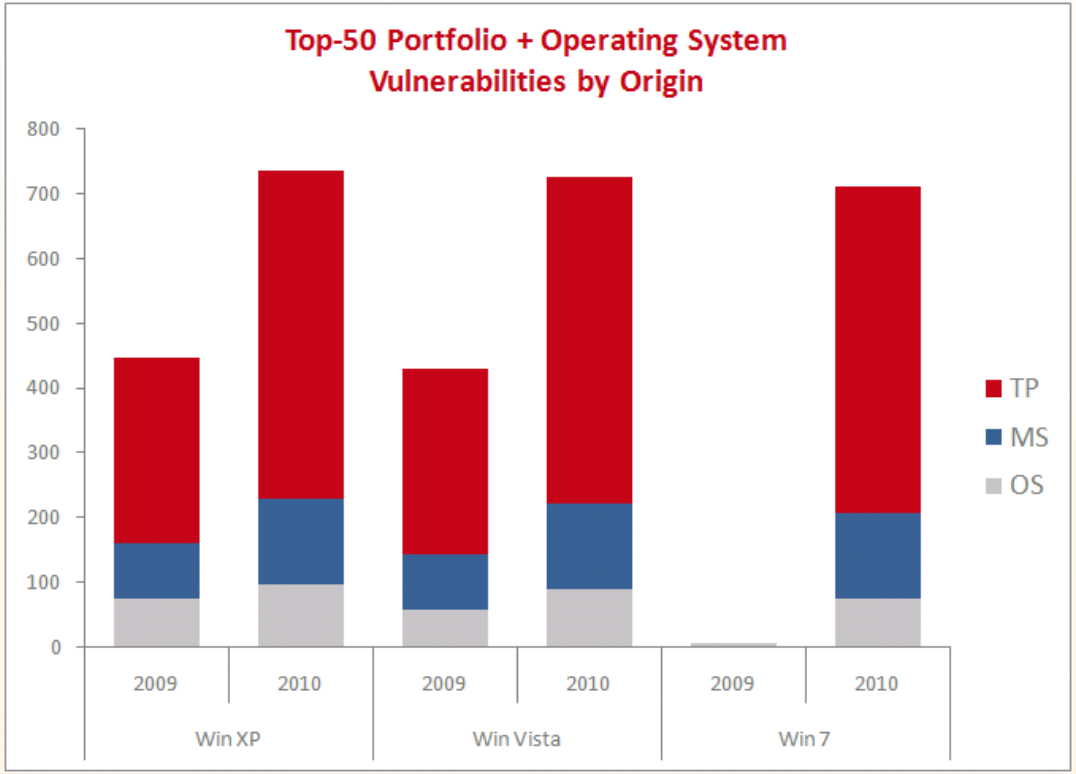
Cybercriminals don't care

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:

- **3.8** 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

+

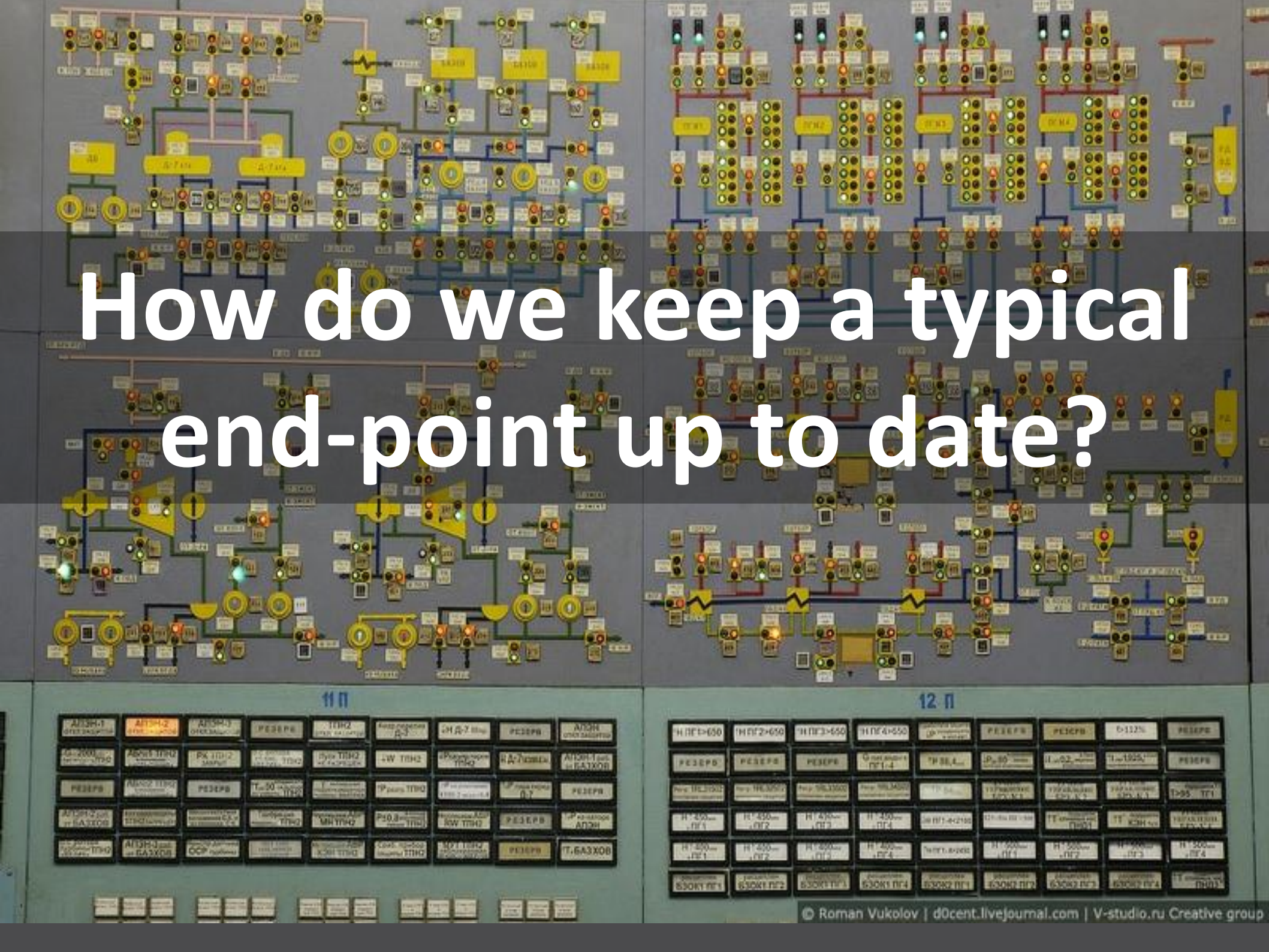
Advisories	163
Vulnerabilities	729

Advisories	153
Vulnerabilities	722

Vulnerabilities -1.0%

Advisories	148
Vulnerabilities	709

Vulnerabilities -2.7%

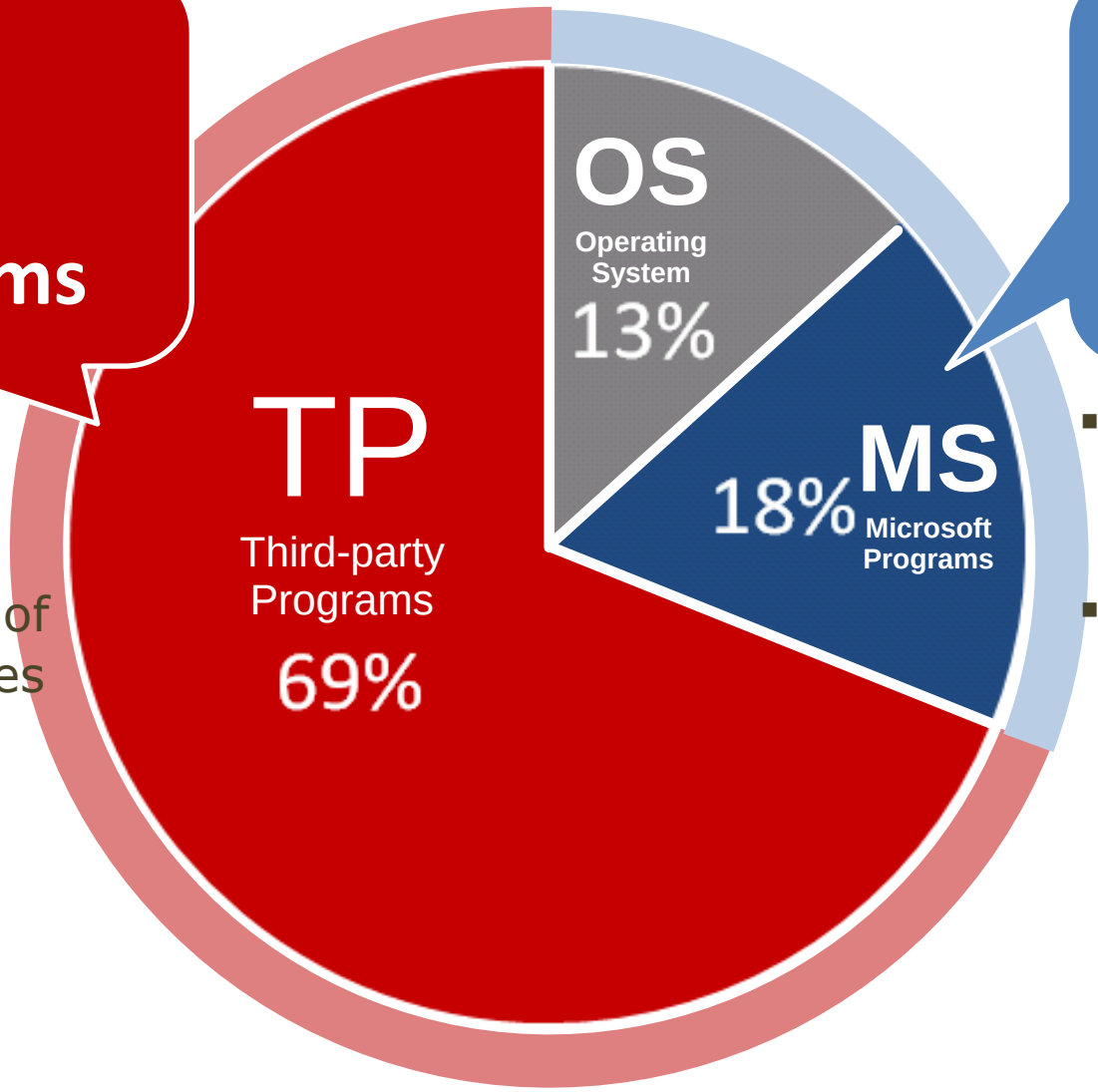

How do we keep a typical end-point up to date?
11 П
12 П
© Roman Vukolov | d0cent.livejournal.com | V-studio.ru Creative group

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

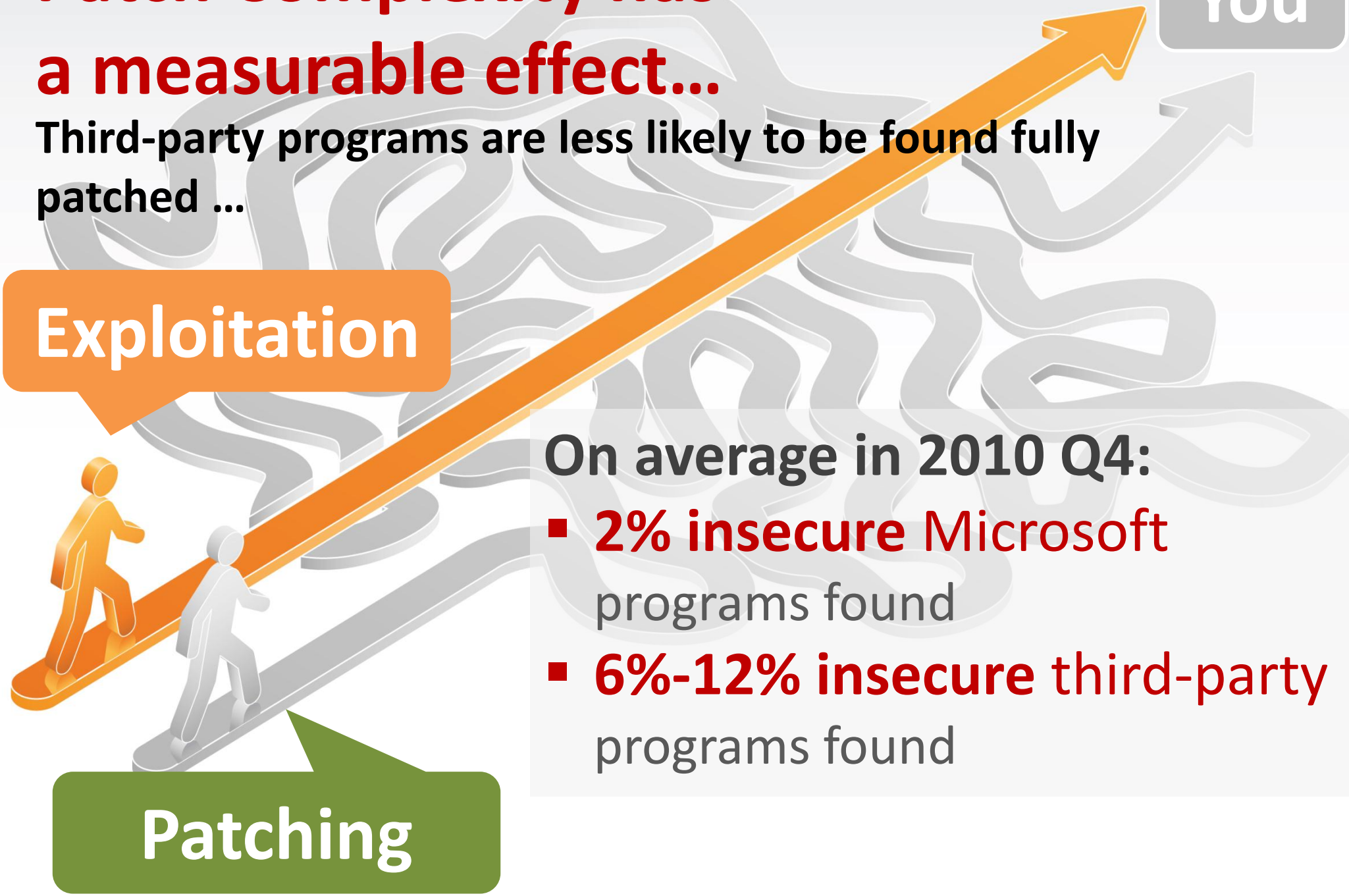
patch available

≠

patch installed

Patch Complexity has a measurable effect…

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



On average in 2010 Q4:

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

Source: Secunia PSI scans 2010/Q4


Are we doomed?

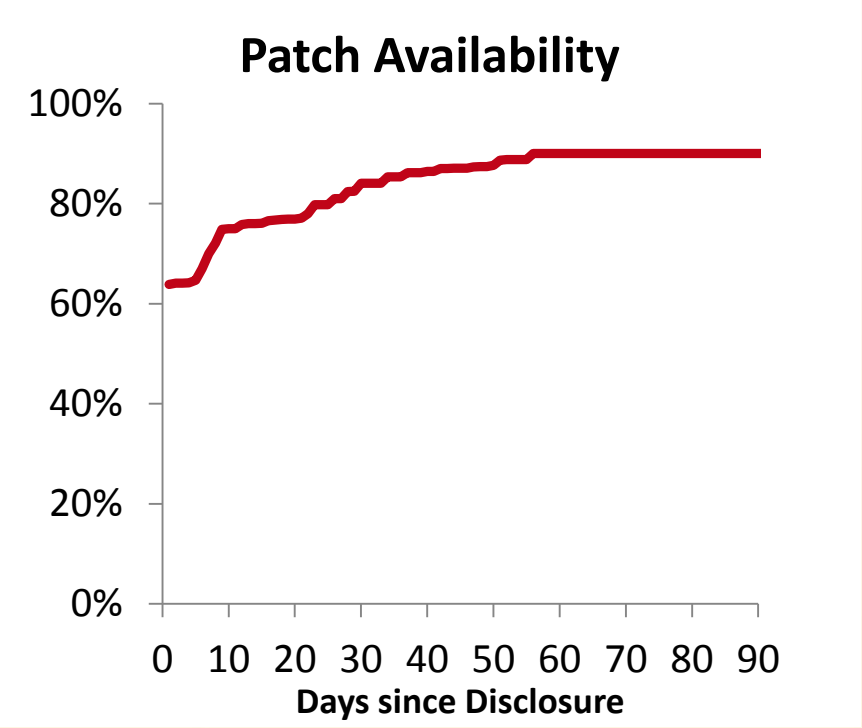
Patches are Available!

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

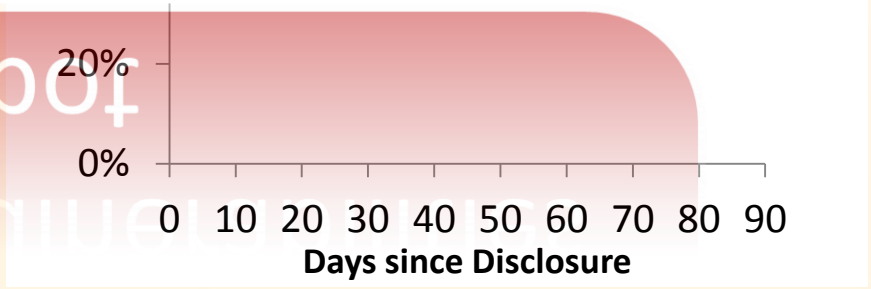


Patches are Available!

Availability of security patches within N days upon vulnerability disclo

Yes YOU can!

.. fix 65% of the vulnerabilities on the spot



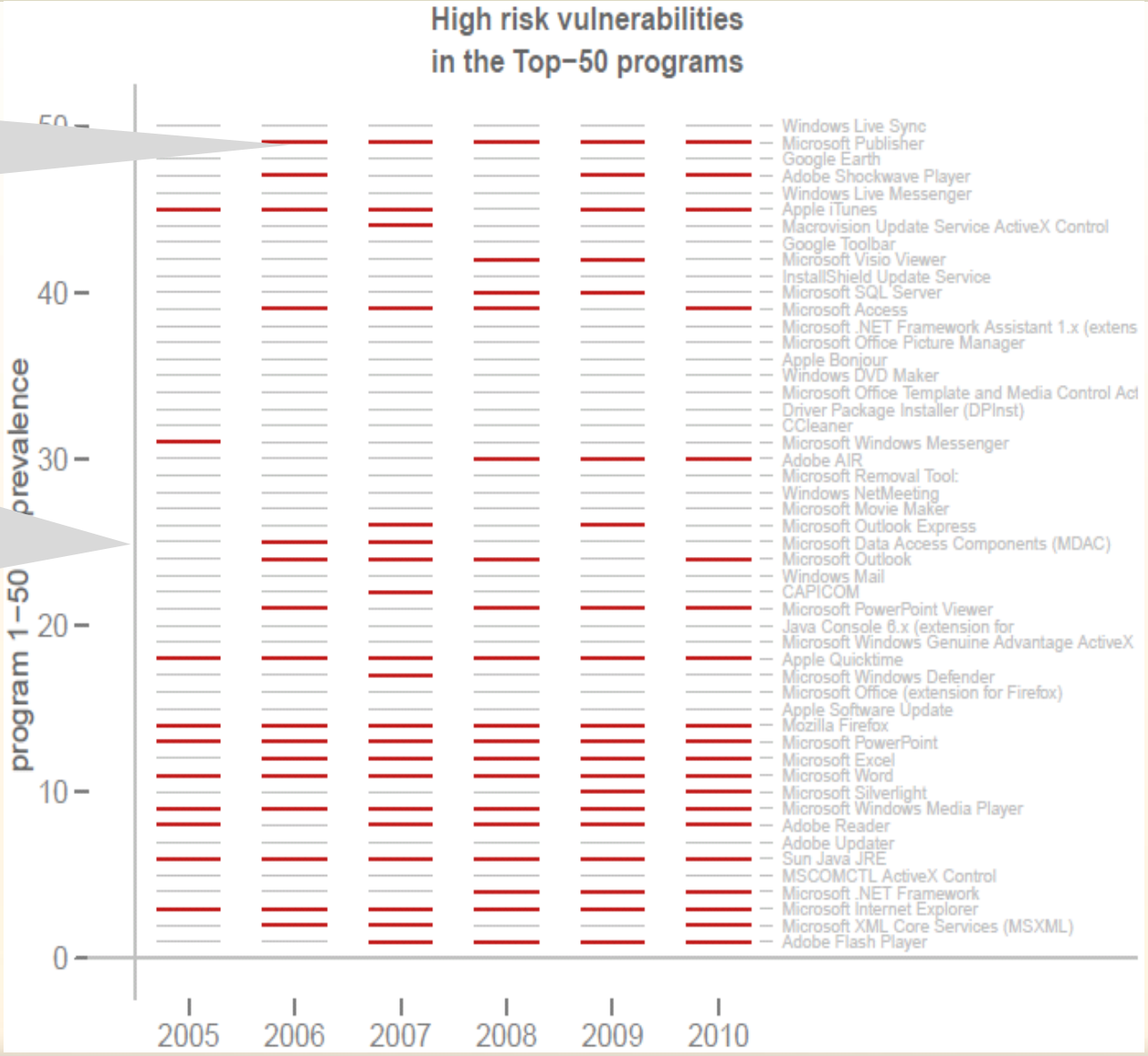
Efficient Patching Strategies

What if you can’t patch all programs?

Chasing a Moving Target

The program had at least one **extremely** or **highly critical** vulnerability in given year

Some programs are vulnerable in several consecutive years; many programs are only vulnerable **in some years** while **not in others**



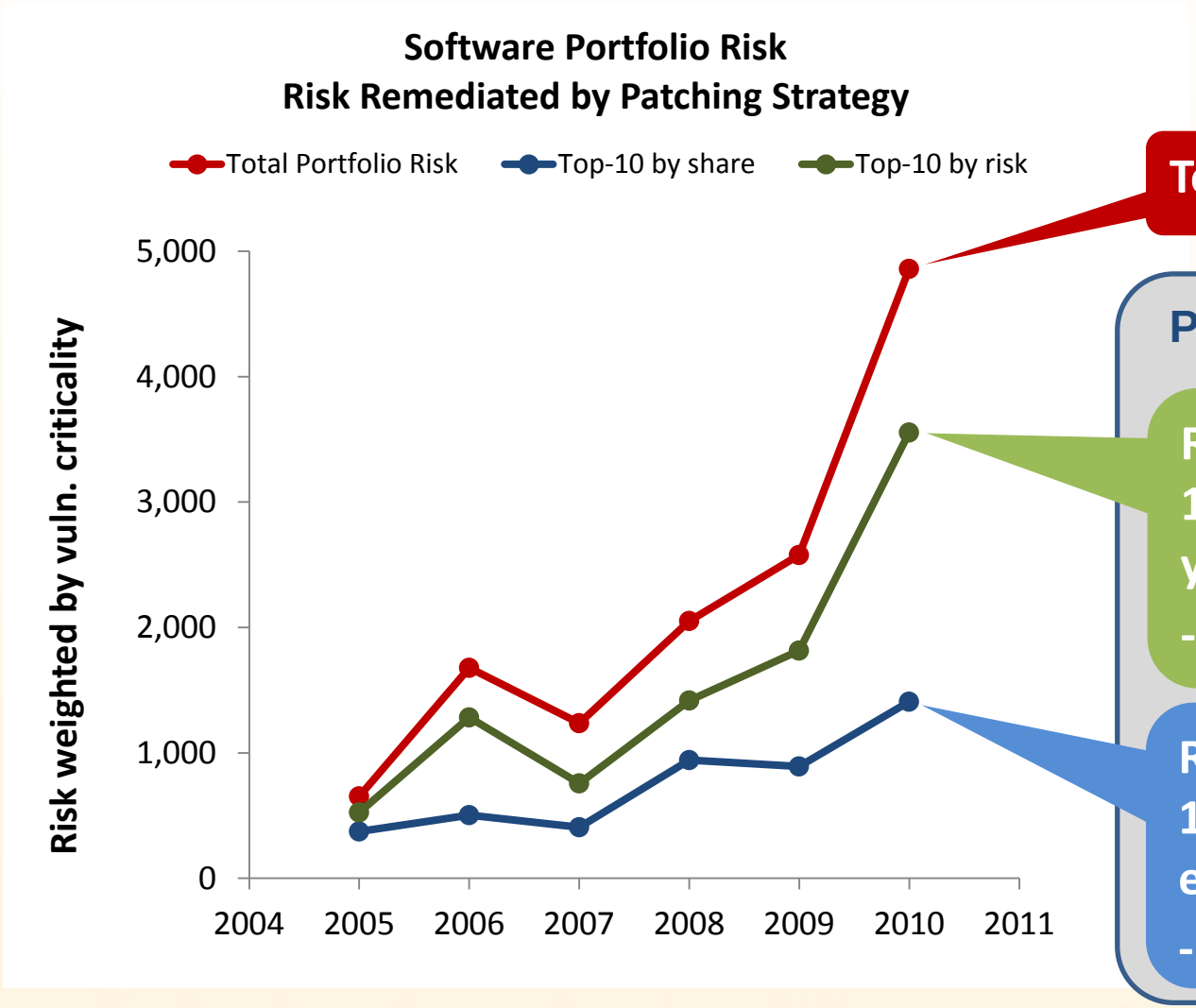
Efficient Patching Strategies

Simulation:

- You have a portfolio of 200 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



Total risk of Top-200 portfolio

Patching 10 programs every year

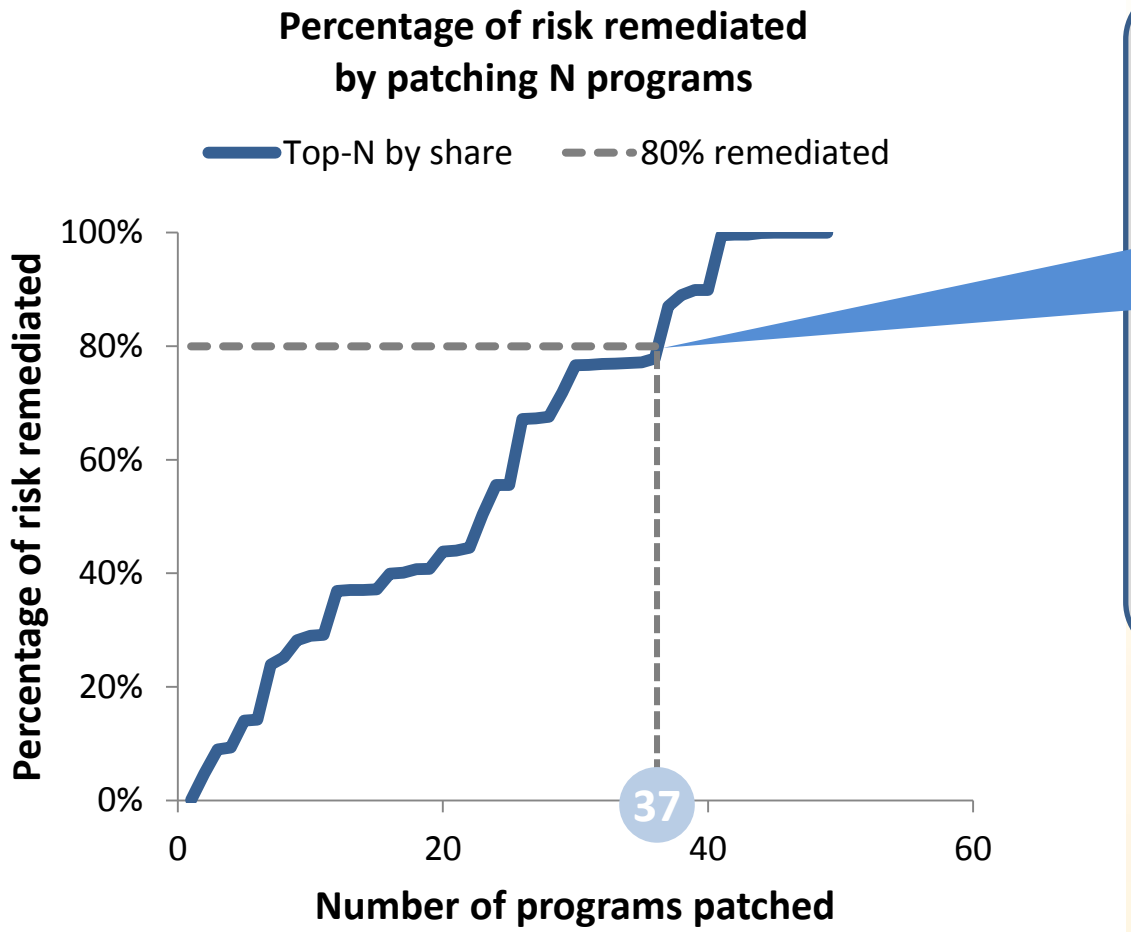
Risk remediated by patching the 10 most critical programs every year:
- Average risk reduction 71%

Risk remediated by patching the 10 most prevalent programs every year:
- Average risk reduction 31%

Weighted Risk: 4 x (extremely+highly critical) + 2x (moderately critical) + 1 x (low + not critical)

Patch Strategies

Statically patching the most prevalent programs



Patching *N* of 200 programs

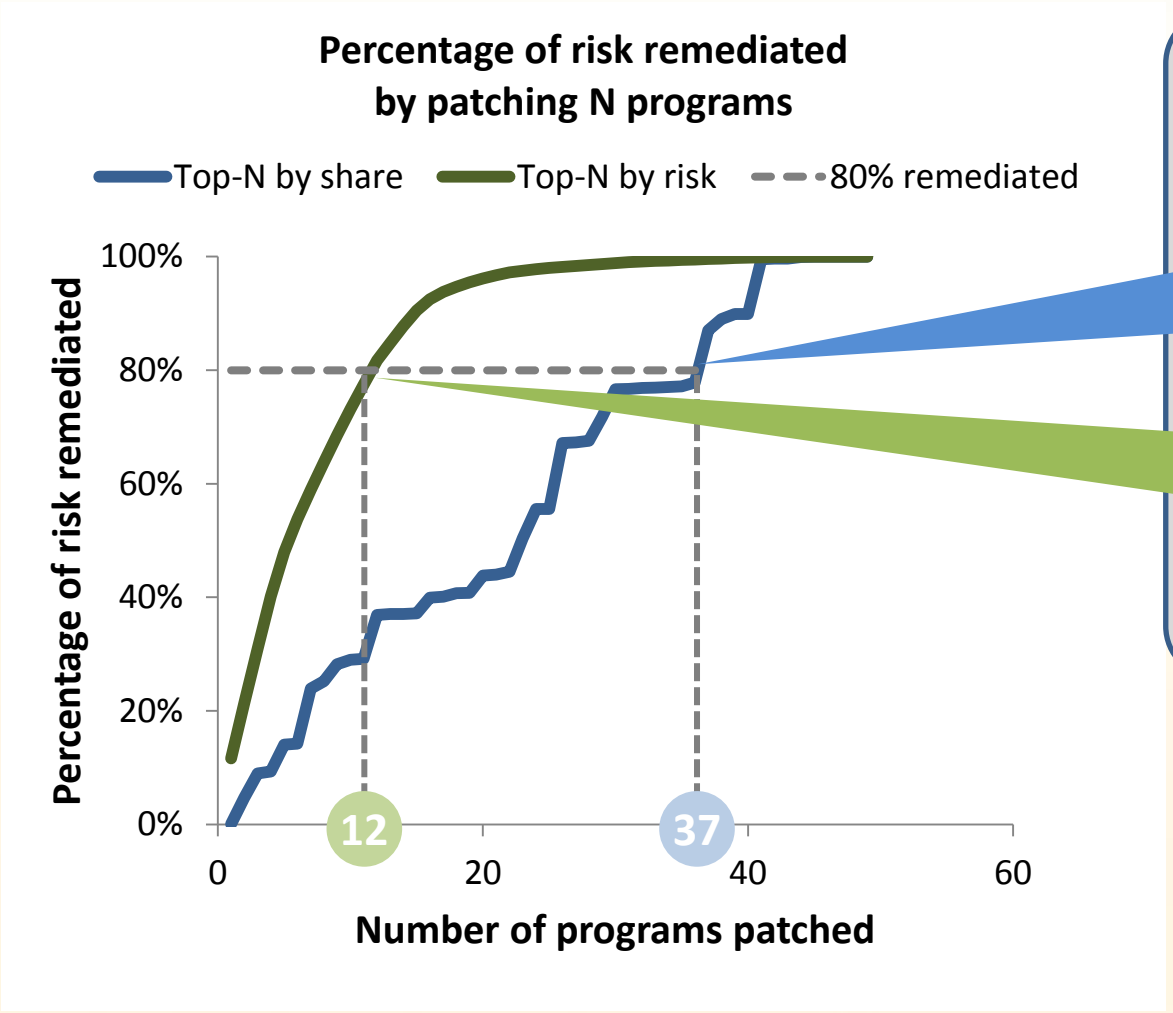
Strategy 1: Static

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

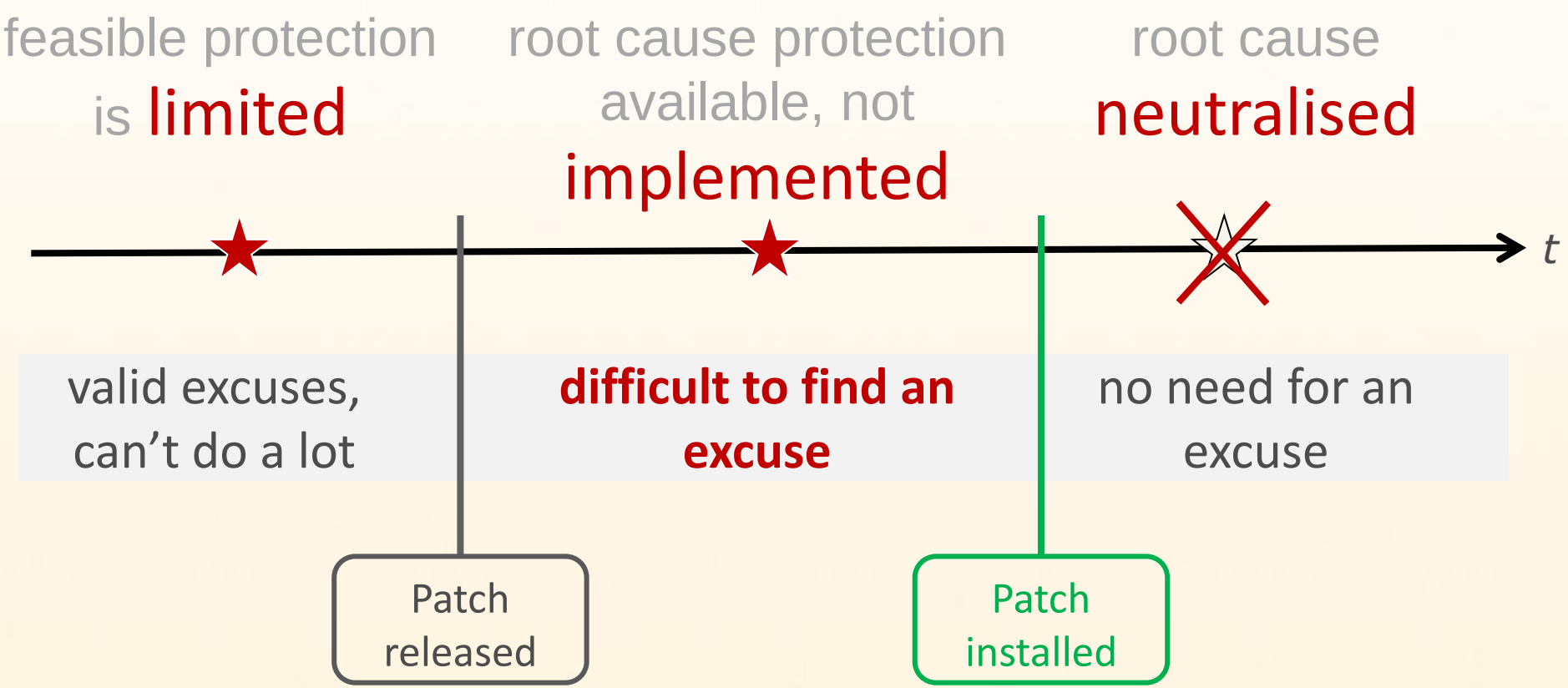
Strategy 2: By Criticality
Risk remediated by patching the *N* most critical programs

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

Responsibility

It depends when you get compromised …

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 1

There is no silver bullet technology

- We need Antivirus, IDS/IPS, …

  However, we also need to be aware of the limitations of these technologies

- Patching should also be prioritised as a primary security measure

  … given its effectiveness to neutralise attacks

Conclusion 2

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
Stay Secure

- 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