How Can a CIO Secure a Moving Target with Limited Resources?

Dr. Stefan Frei

Research Analyst Director

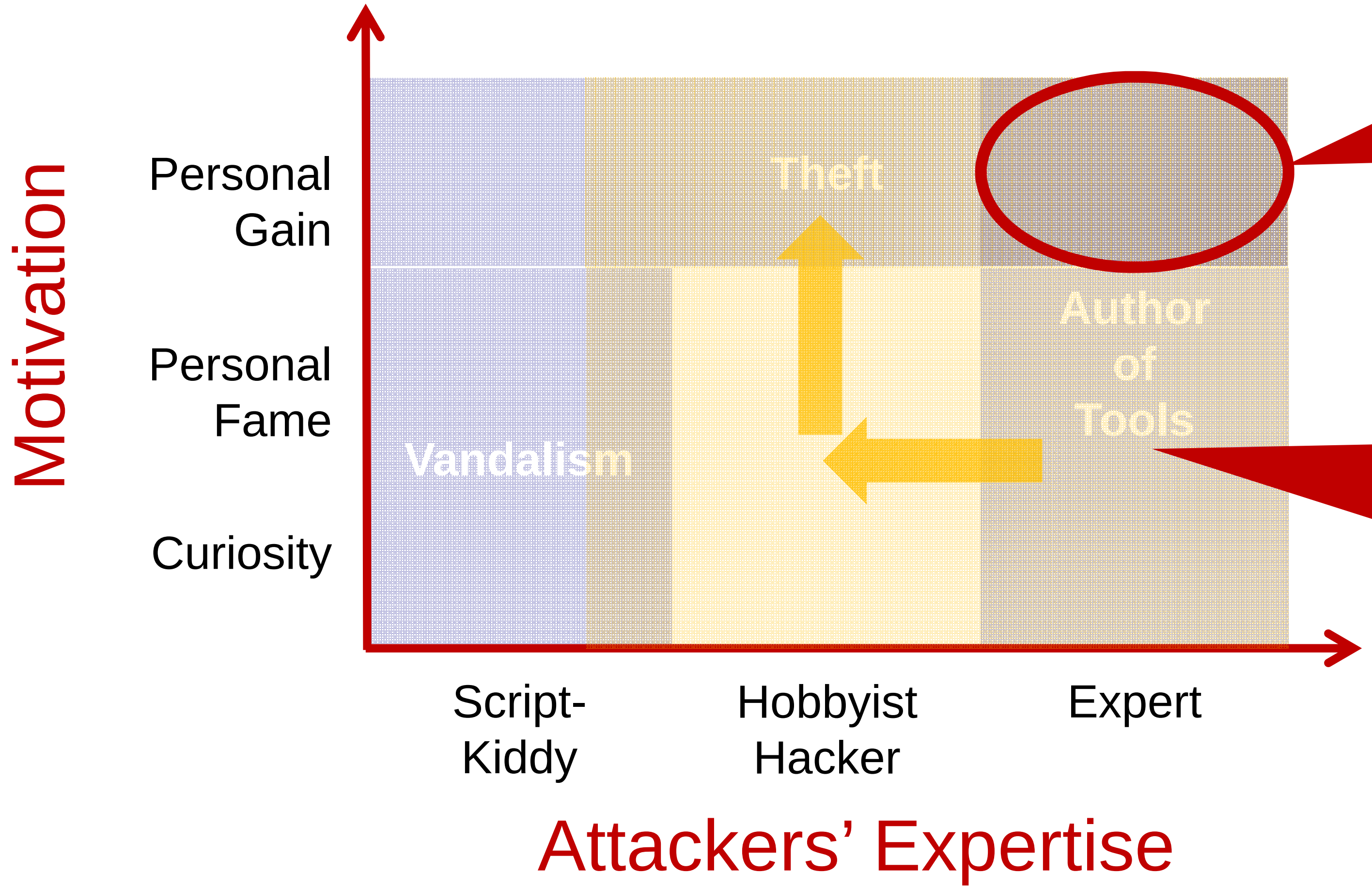
Secunia

Session ID: SPO2-302

Session Classification: Intermediate

RSACONFERENCE2012

Know your Enemy
The Changing Threat Environment



Fastest growing segment

Tools created by experts now used by less-skilled criminals, for personal gain

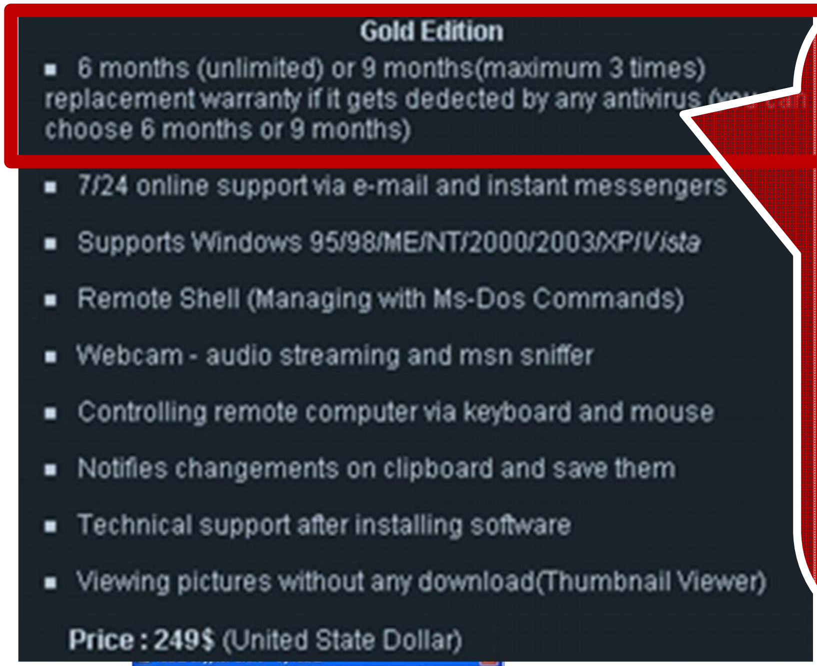
Availability of Malware Tools
leads to ..

High degree of attack automation

+

More opportunistic attacks

Malware as a Service (MaaS)

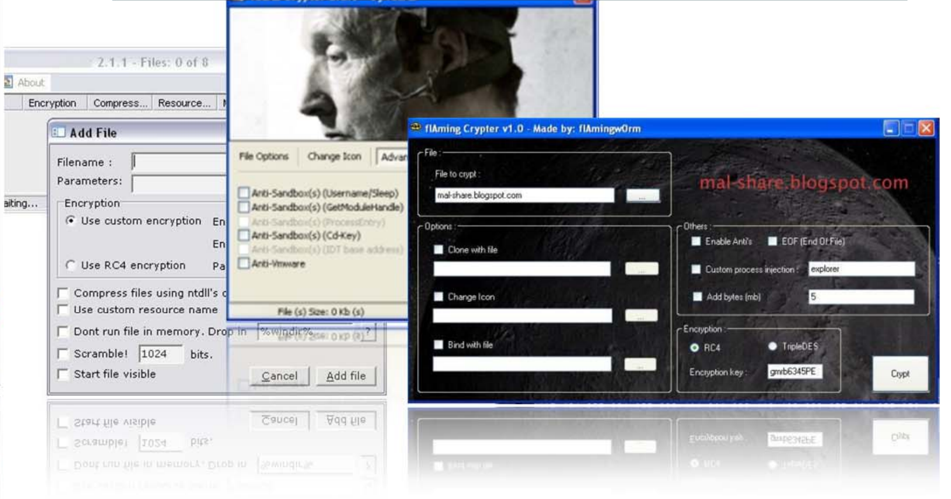


Gold Edition

- 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 messengers
- 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



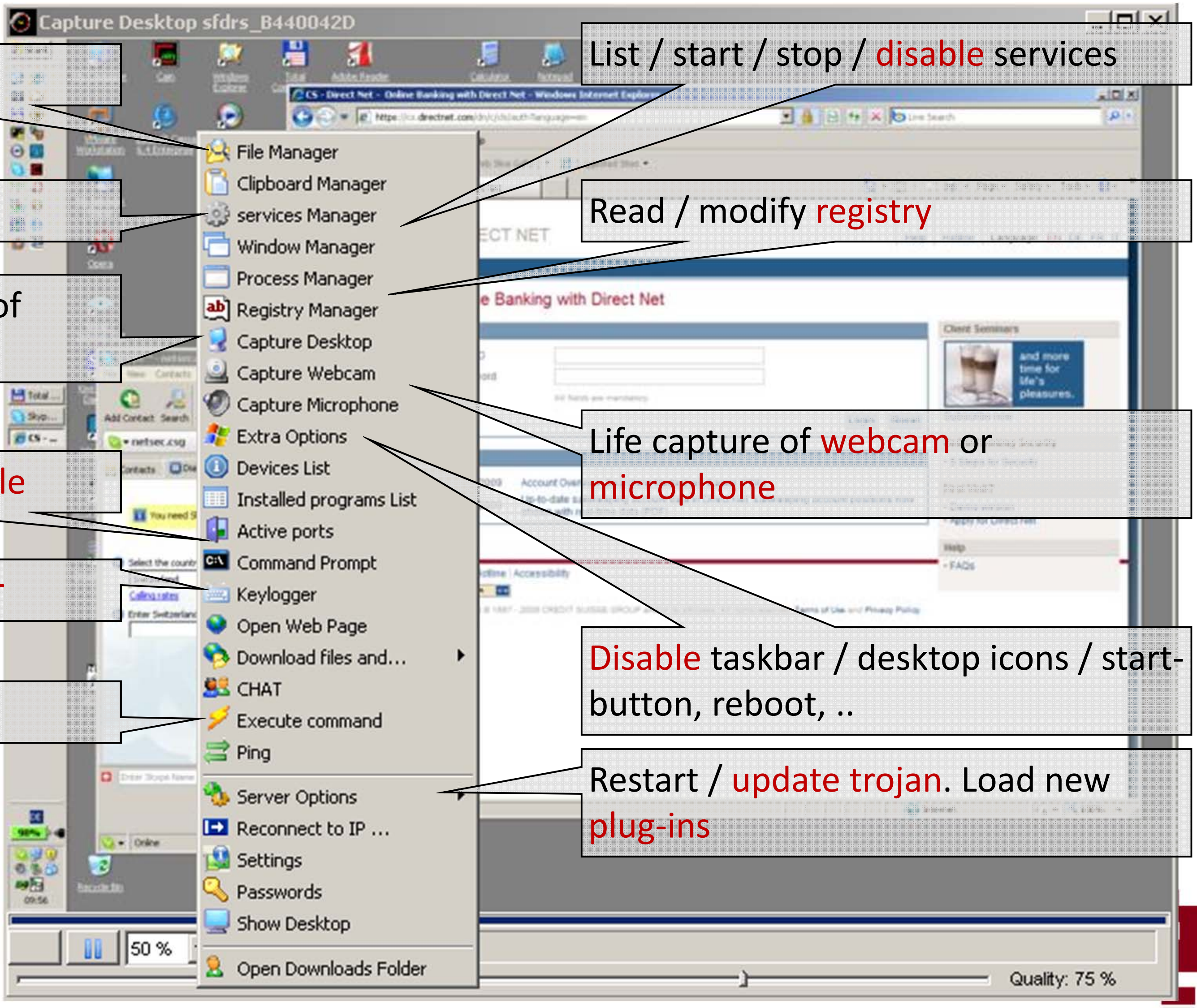
Source: www.turkojan.com

Malware Construction Kit
Live Demonstration

We “trojanize” **Windows Minesweeper** using an off-the-shelf malware construction kit

Absolutely no coding expertise required!

Full Remote Control..



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

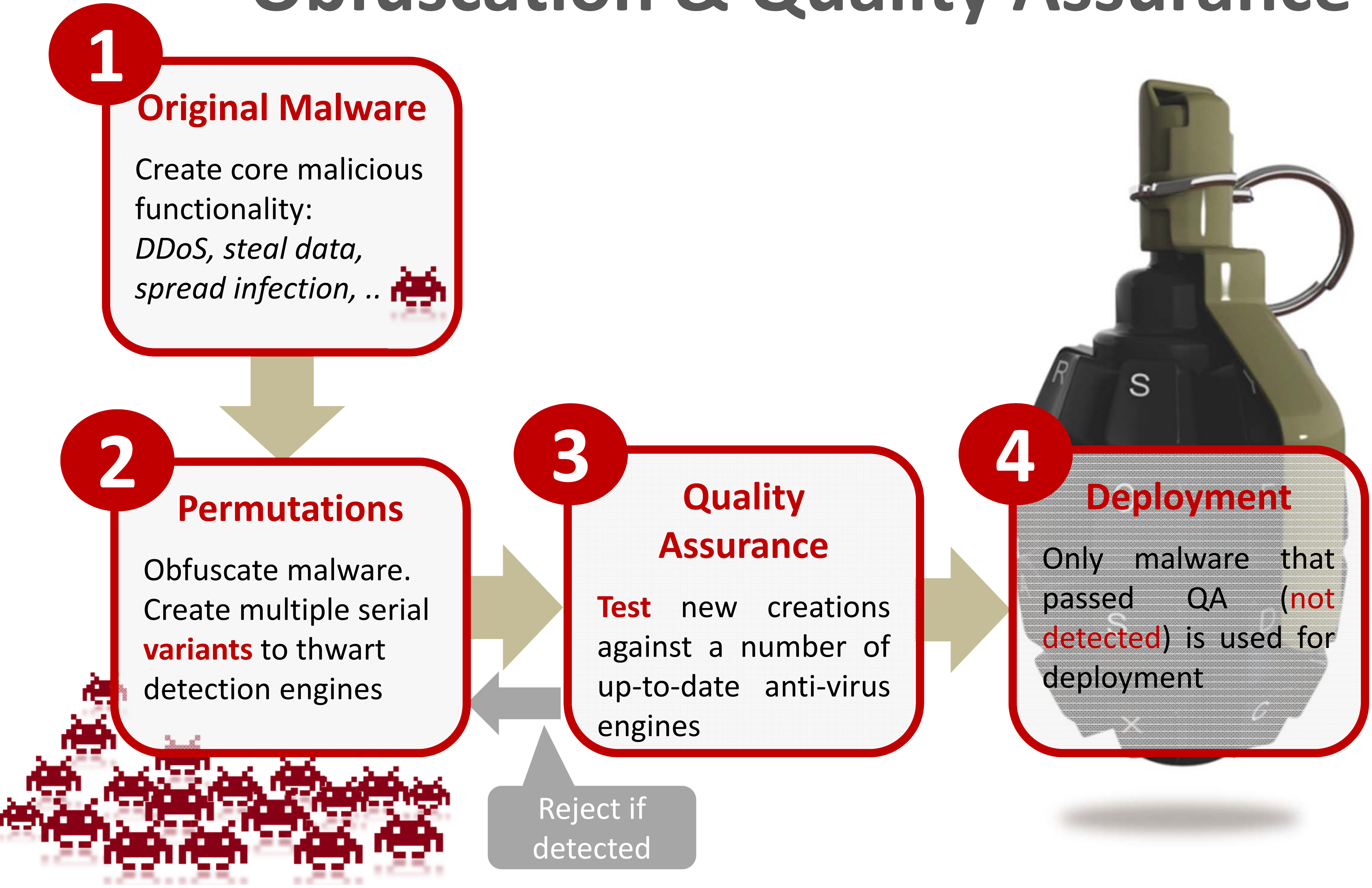
Life capture of webcam or microphone

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

Restart / update trojan. Load new plug-ins

Malware Development Process

Obfuscation & 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

Reject if detected

4 **Deployment**

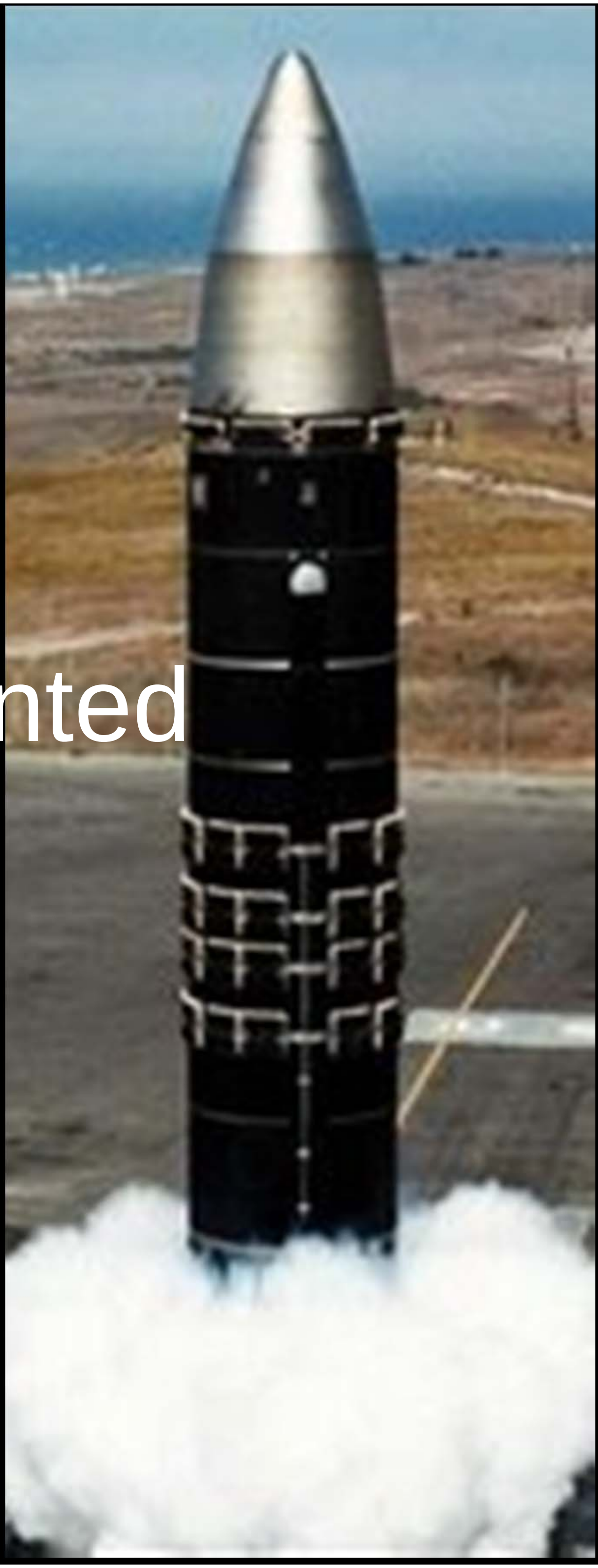
Only malware that passed QA (not detected) is used for deployment

An Arms Race …

286 million

virus samples counted in 2010

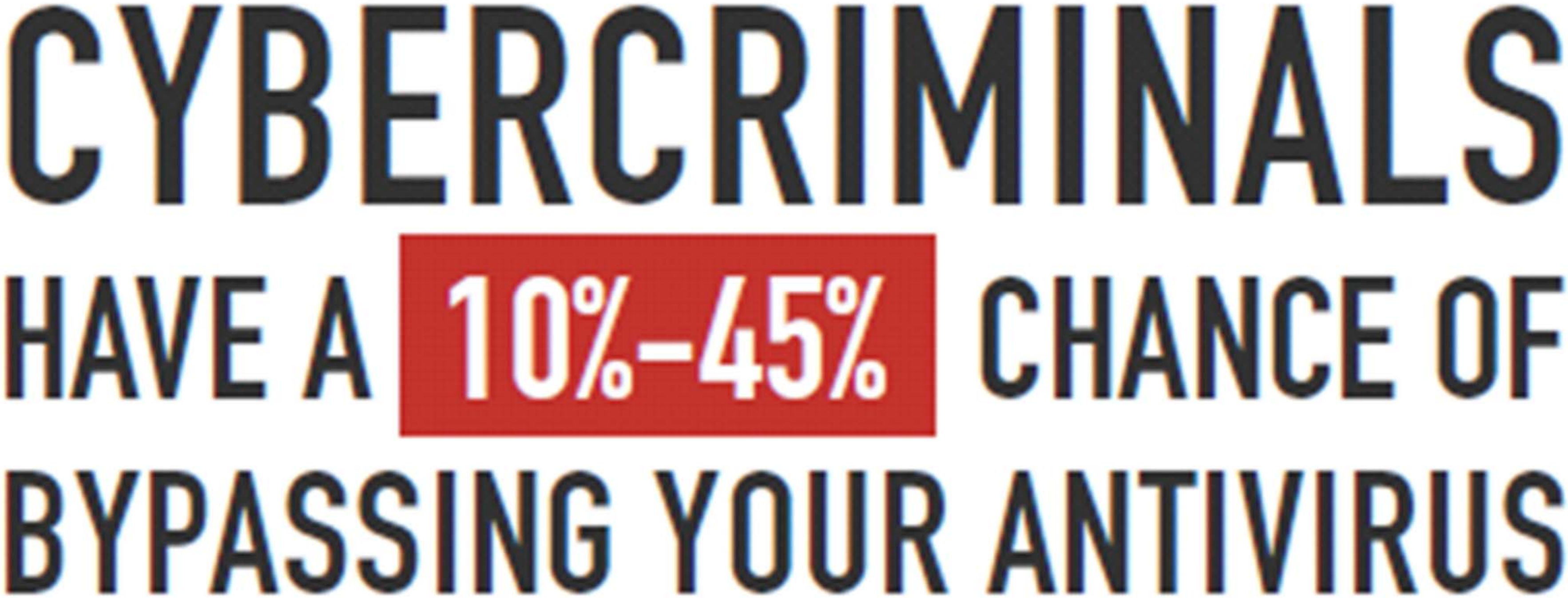
783,562	samples / day
32,648	samples / hour
544	samples / minute
9	samples / second



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

Limitations of traditional defense

We are to loose this Arms Race ..



CYBERCRIMINALS HAVE A 10%–45% CHANCE OF BYPASSING YOUR ANTIVIRUS

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

NSS Labs Anti-Malware Test Report 2010Q3
Damballa on Darkreading, 2010

From a Criminal's Perspective

#Hosts x #Vulnerabilities

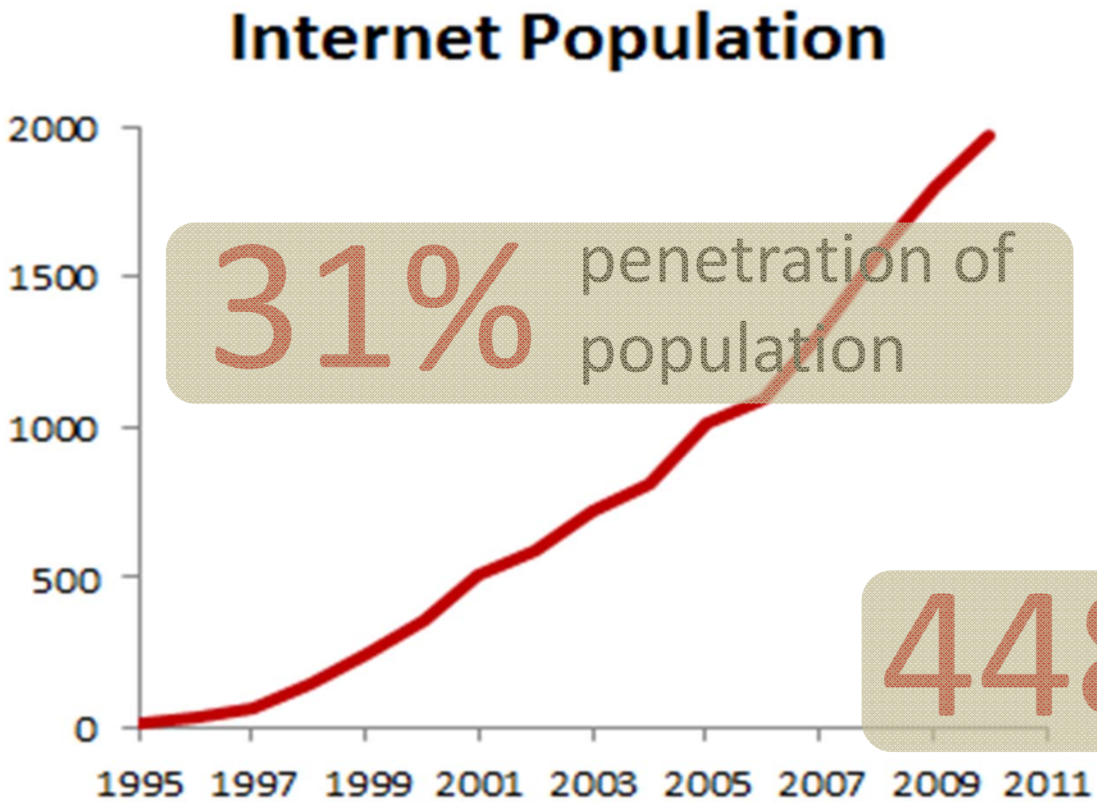
=

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: http://www.internetworldstats.com

2,095 Million potential victims..

End-points are increasingly targeted

1. End-point 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

2. End-points are **difficult** to secure

   Highly dynamic environment and unpredictable usage patterns by users

3. A **single vulnerable program** is enough

   Cybercriminals only need a single vulnerable program to compromise the entire system

From a Criminal's Perspective

#Hosts x #Vulnerabilities

=

Opportunity

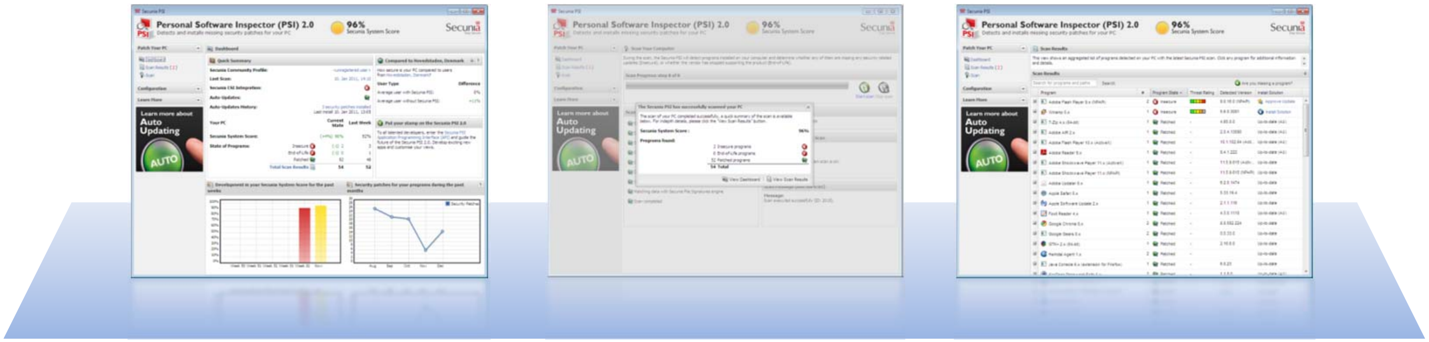
Analysis

What does an end-point look like?

Data: Scan results from more than 4.8 Mio users of the Secunia Personal Software Inspector PSI

Secunia PSI is a lightweight scanner to

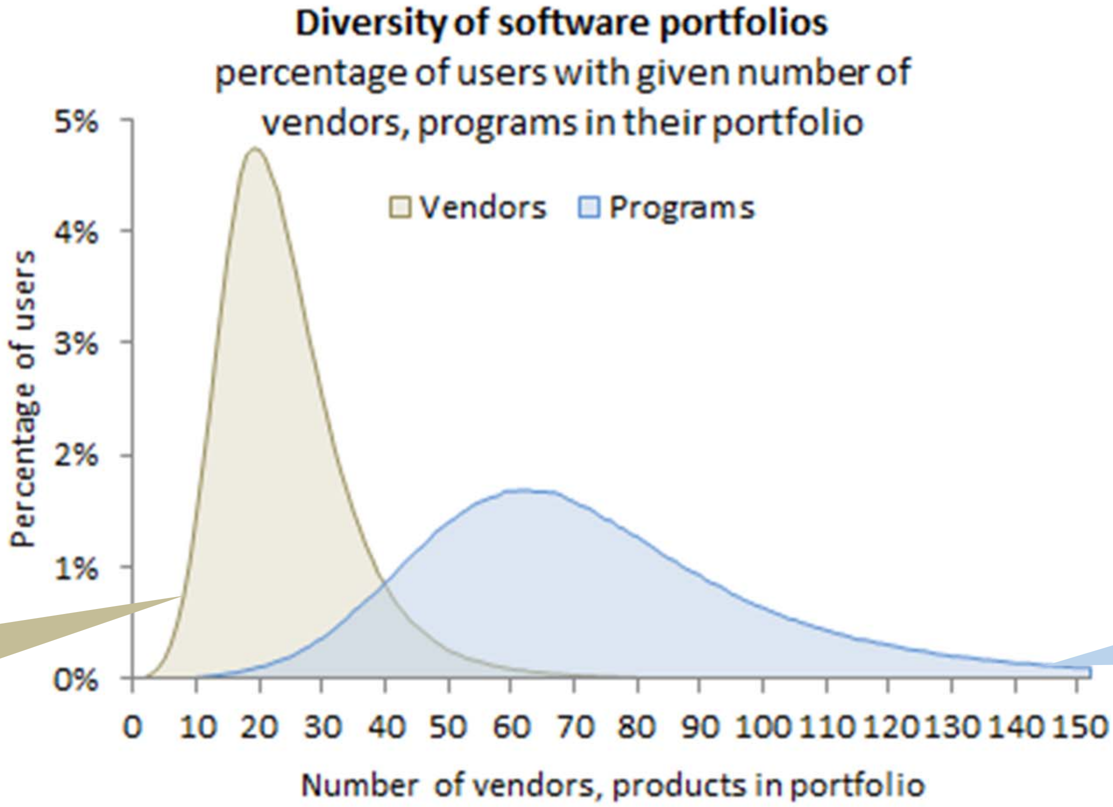
- enumerate and identify insecure programs
- automatically install missing patches


Personal Software Inspector (PSI) 2.0
96%
Secunia System Score
Secunia
Learn more about Auto Updating
AUTO

- Free for personal use http://secunia.com/psi

WHAT'S ON YOUR PC?

MORE THAN 66 PROGRAMS FROM 22 COMPANIES


Diversity of software portfolios
percentage of users with given number of vendors, programs in their portfolio

Distribution of #vendors

Distribution of #programs

The Top-50 Software Portfolio ..

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

28 Microsoft and 22 third-party (non MS) programs from 12 different vendors

12 Vendors

28 Microsoft

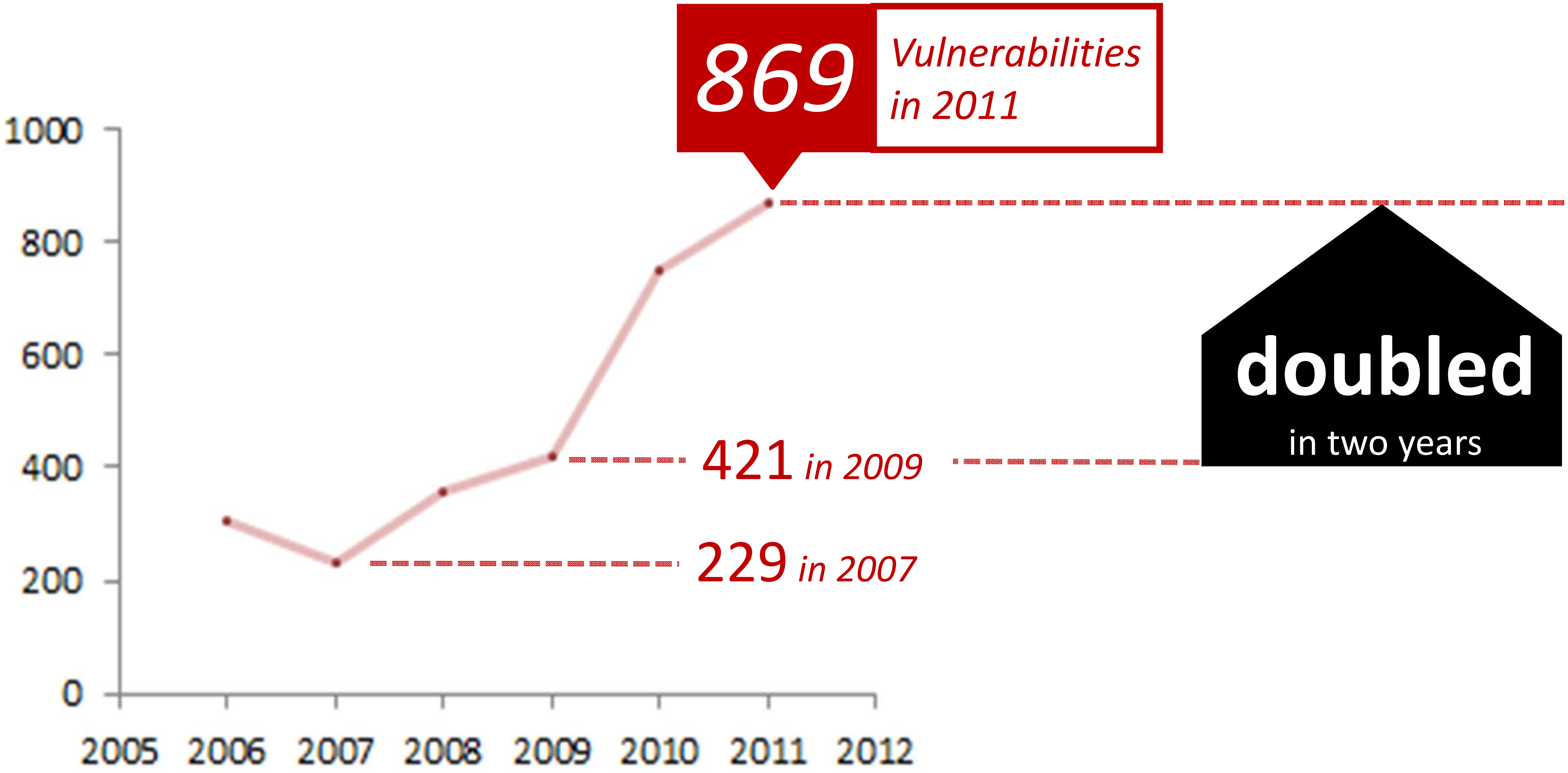
22 Third-party

Top-50 Portfolio as of December 2011

An alarming trend ..

in # of end-point vulnerabilities

Number of vulnerabilities continuously increased since 2007



869 *Vulnerabilities in 2011*

doubled

in two years

421 *in 2009*

229 *in 2007*

A relevant trend ..

in criticality and type of vulnerabilities

800+

Vulnerabilities

of which

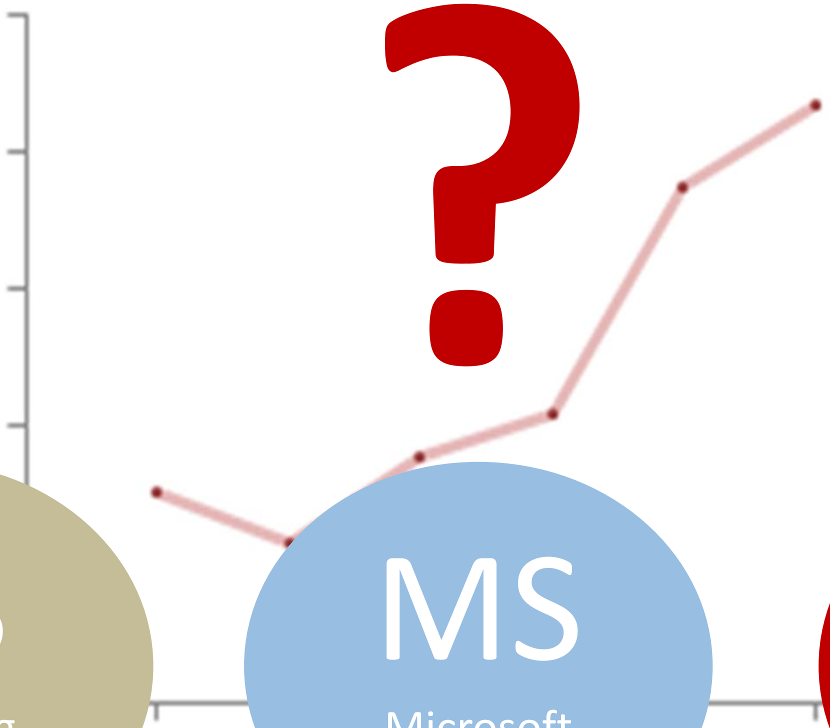
>50%

PROVIDE SYSTEM ACCESS TO ATTACKER

ARE HIGHLY CRITICAL

ARE EXPLOITABLE REMOTELY

What is the source of this increasing trend?



OS

Operating System

MS

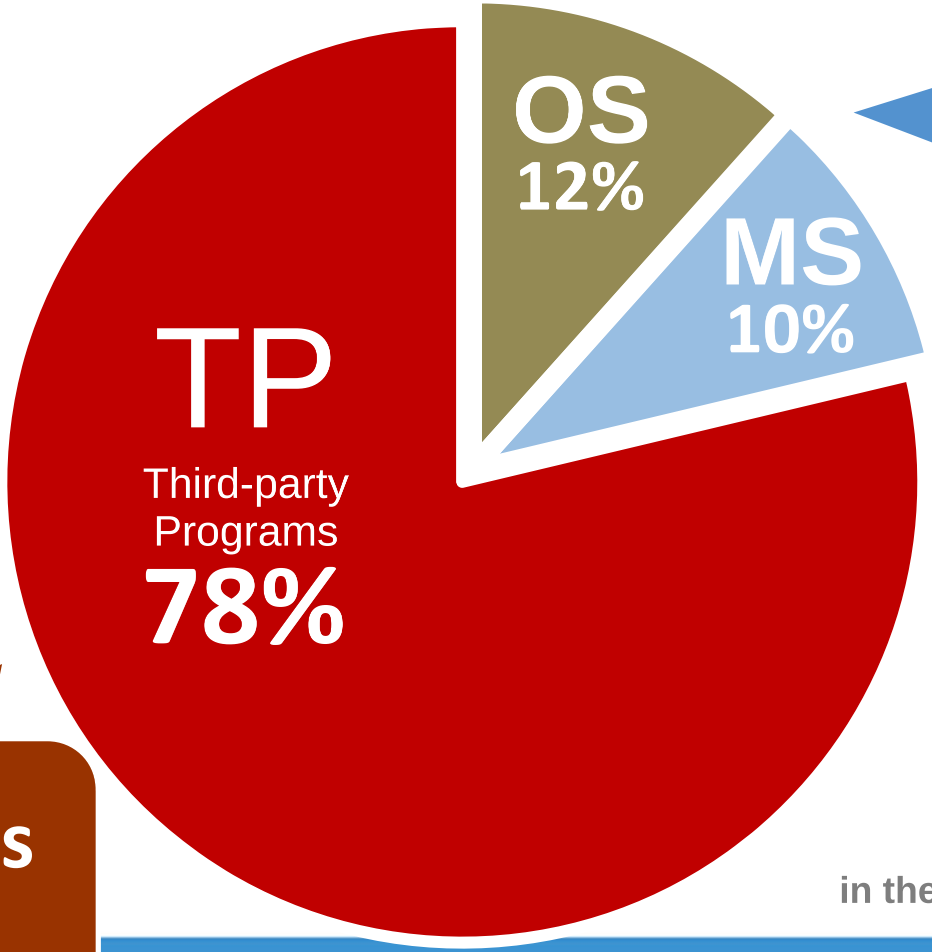
Microsoft Programs

TP

Third-party Programs

It is third-party programs

Non-Microsoft programs are found to be almost exclusively responsible for this increasing trend



What you patch

Cybercriminals don’t care

Origin of vulnerabilities
in the Top-50 Portfolio as of Dec 2011

The Operating System
& Top-50 Software Portfolio

Top 50 Portfolio

2011

+

Microsoft Windows xp

Vulnerabilities 870

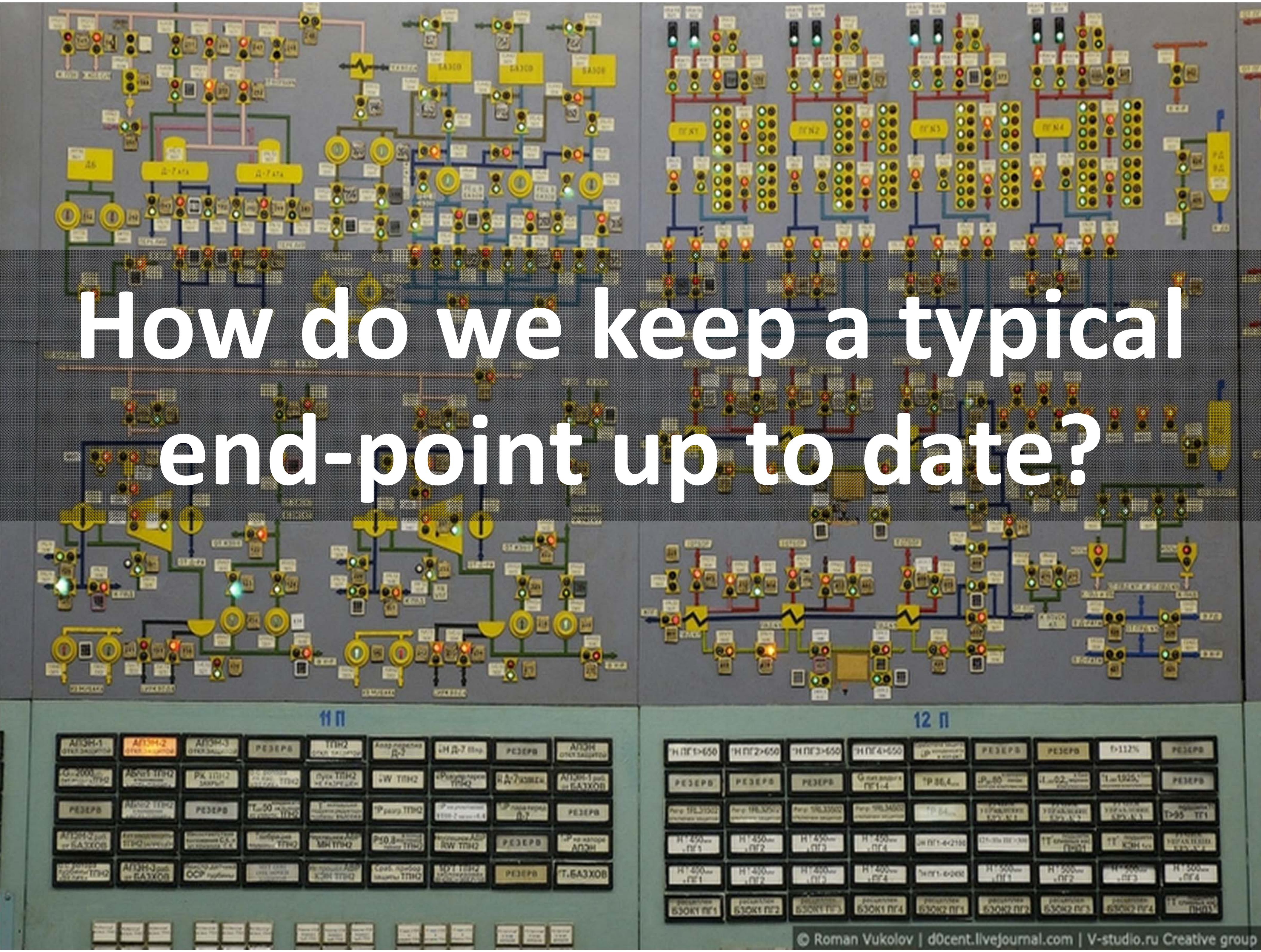
Windows Vista

Vulnerabilities 867

Windows 7

Vulnerabilities 869

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



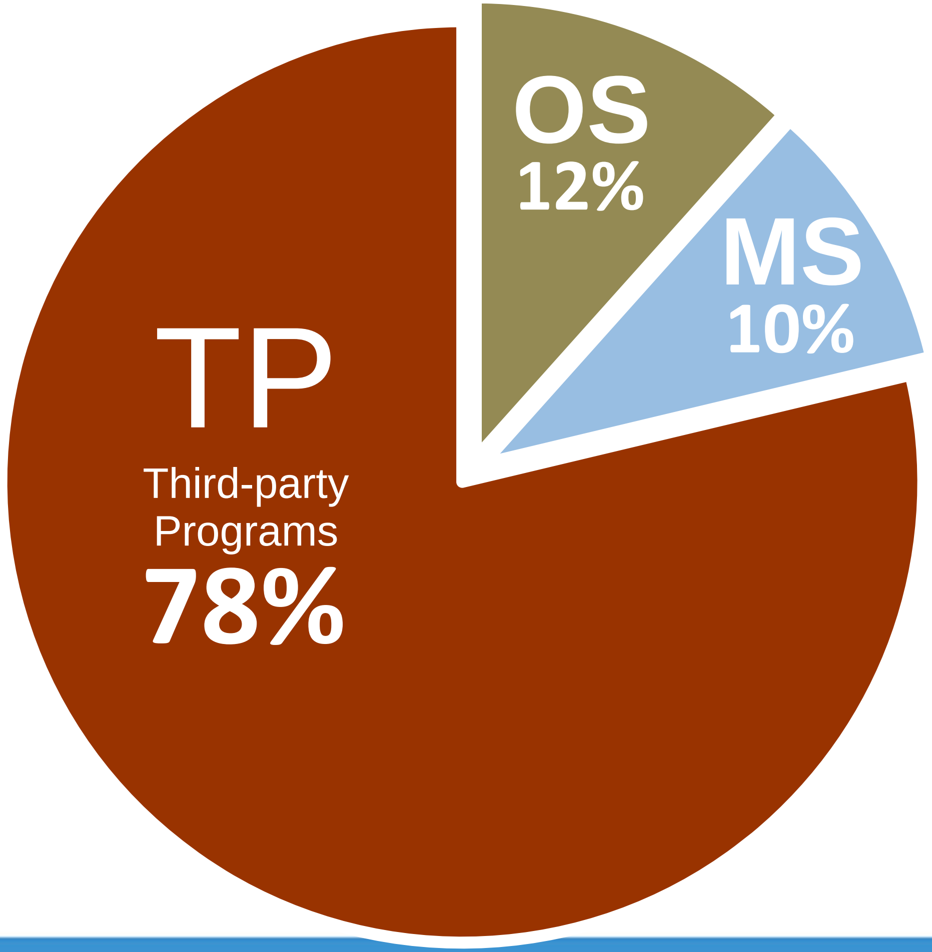
© Roman Vukolov | d0cent.livejournal.com | V-studio.ru Creative group

Complexity hurts

12 different update mechanisms ..

11 Update Mechanisms

TO PATCH
22 third-party programs
fix **78%** of the vulnerabilities



1 Update Mechanism

TO PATCH
OS+28 Microsoft programs
fix **22%** of the vulnerabilities

Cybercriminals know

patch available

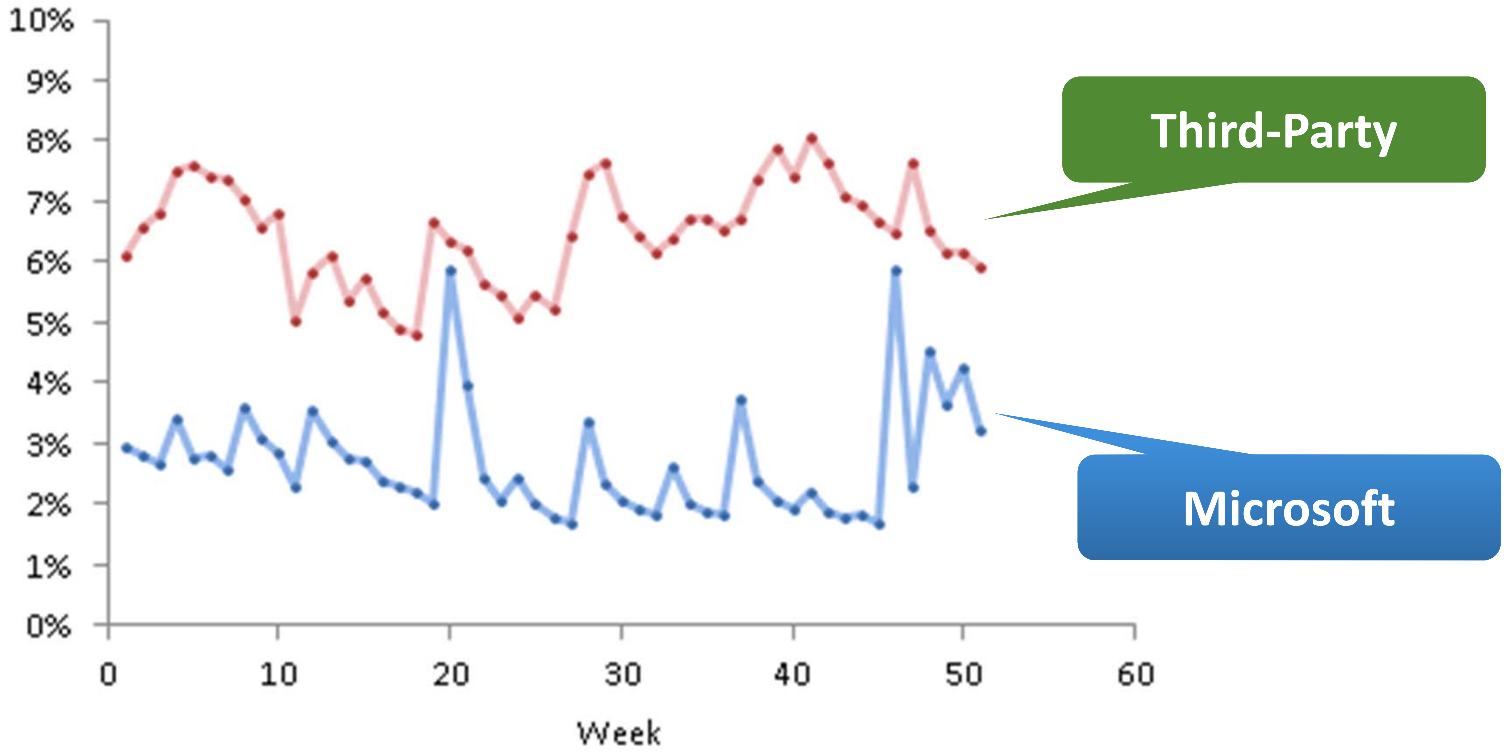
≠

patch installed

Patch Complexity ..

has a measurable effect on security

Percent of unpatched programs



2011 average

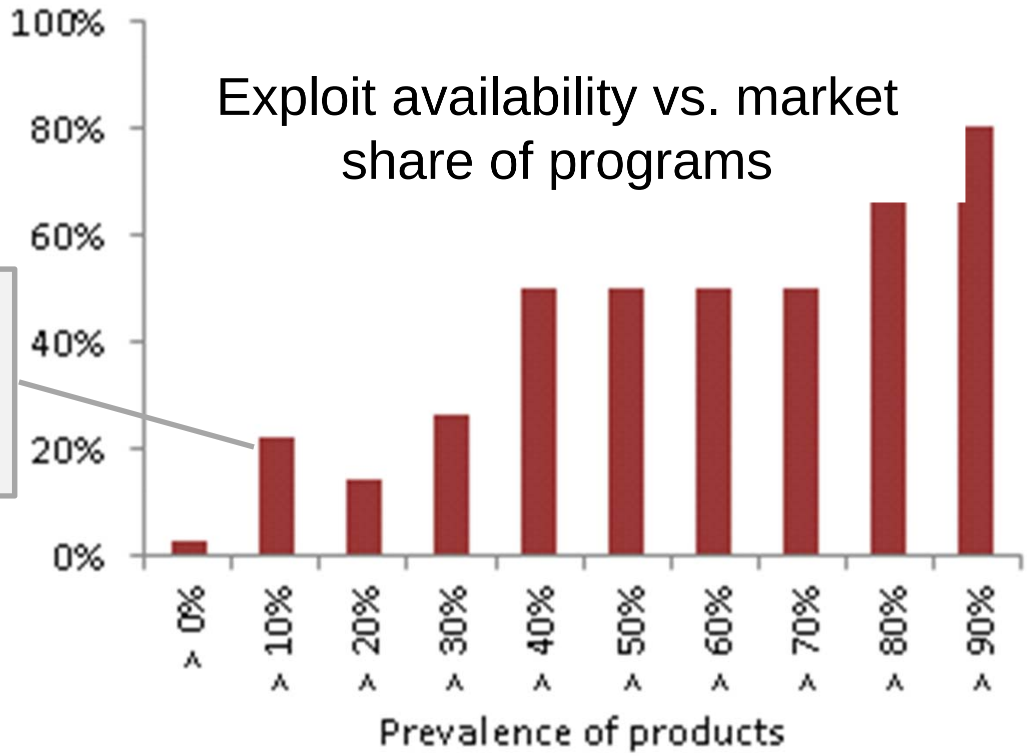
2.7 % insecure Microsoft programs
6.5 % insecure Third-Party programs

You can’t hide

Even rare programs have exploits

FALLACY Programs with low market share are not exposed as no exploits exist

22% of the programs with 10-20% market share have exploits



Are we doomed?

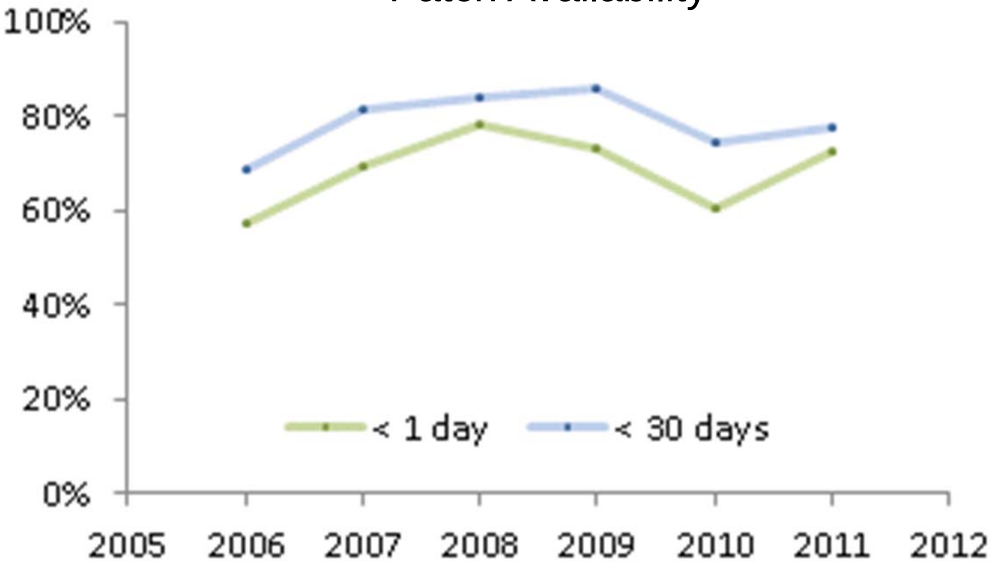
The Good News

most patches are available on time!

72%

of the patches are available on the day of vulnerability disclosure

Patch Availability



Cybercriminals
.. don't need zero-day exploits!

Malware propagation methods:

< 1% of the attacks had no patch available at the day of attack (zero-day attack)

Microsoft SIR 11 Report 1H2011

Cybercriminals always find more than enough opportunity in unpatched and well understood program vulnerabilities

Instant patching of all programs is a major challenge

What patching strategy yields the largest risk reduction **with limited resources available** ?

Simulation

Static vs. Dynamic Patching

Say you have a portfolio of the 200 most prevalent programs

On average, how many programs do you need to patch every year to get a 80% risk reduction?

Static Approach

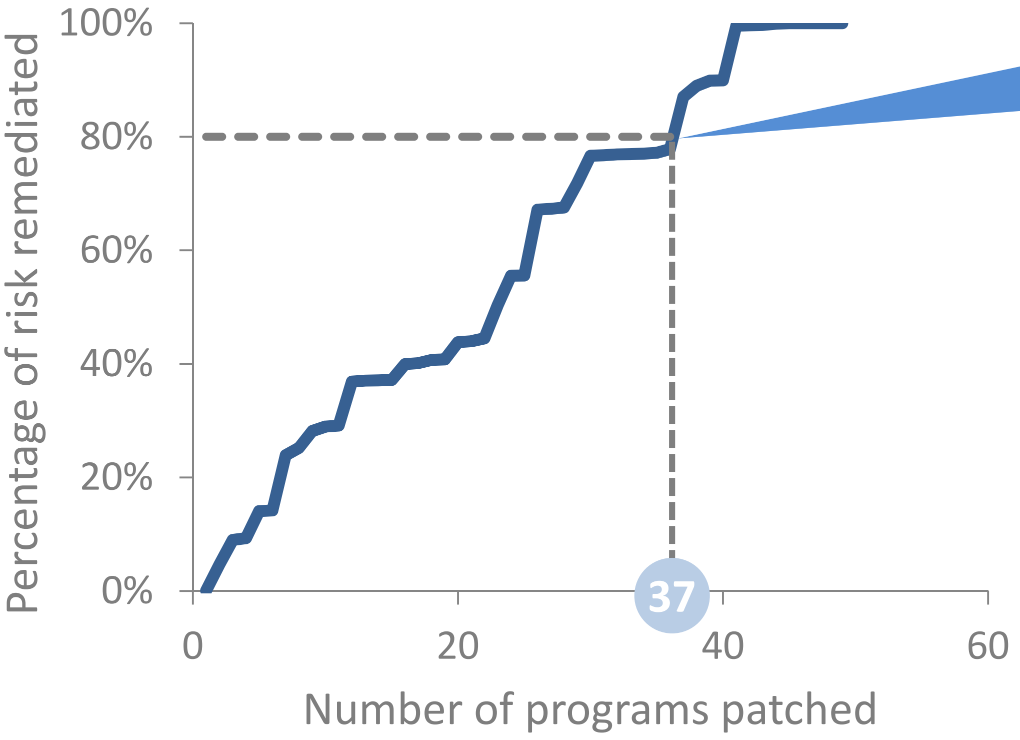
Patch the ***N*** **most prevalent** programs every year

Dynamic Approach

Patch the ***N*** **most critical** programs every year

Statically patching
.. the most prevalent programs

Percentage of risk remediated by patching N programs



Patching *N* of 200 programs

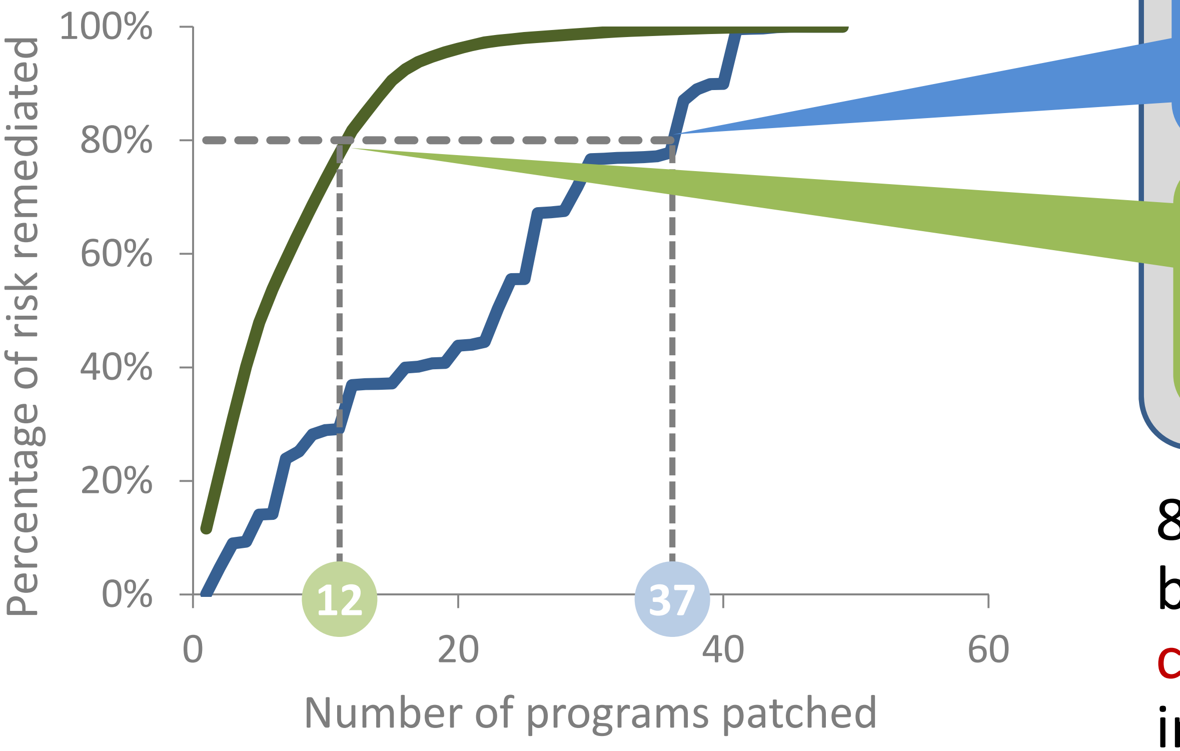
Strategy 1: Static

Risk remediated by patching the *N* most prevalent programs

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

Statically patching
.. the most critical programs

Percentage of risk remediated by patching N programs



Patching *N* of 200 programs

Strategy 1: Static

Risk remediated by patching the *N* most prevalent programs

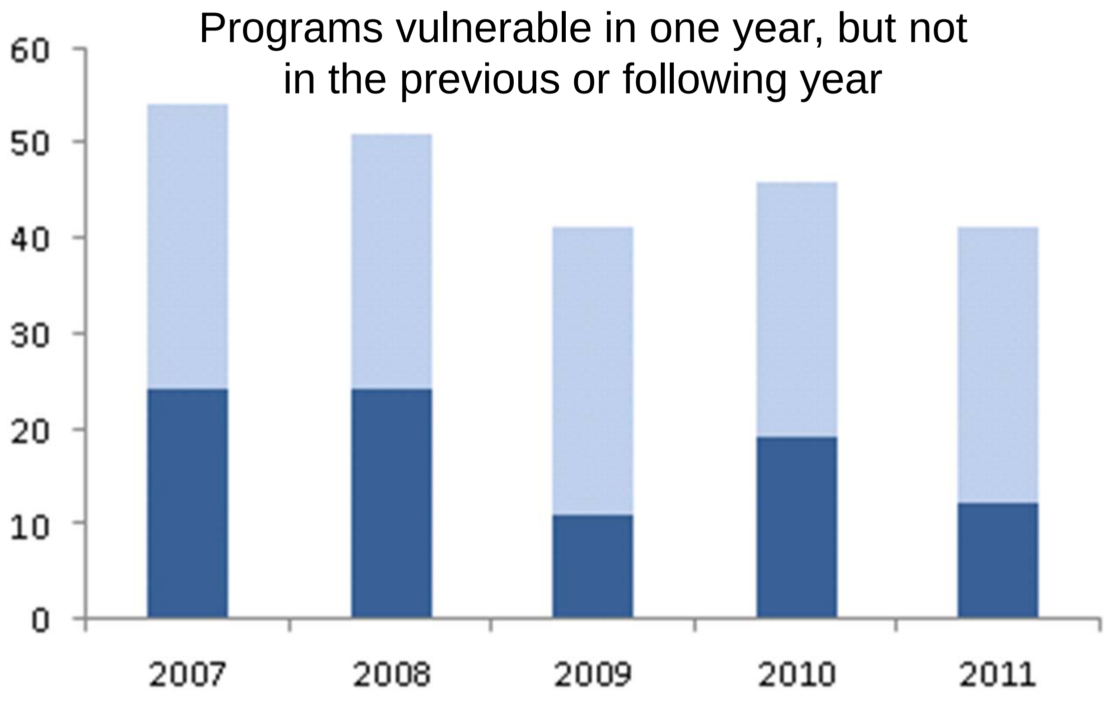
Strategy 2: By Criticality

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

Why?

.. chasing a moving target



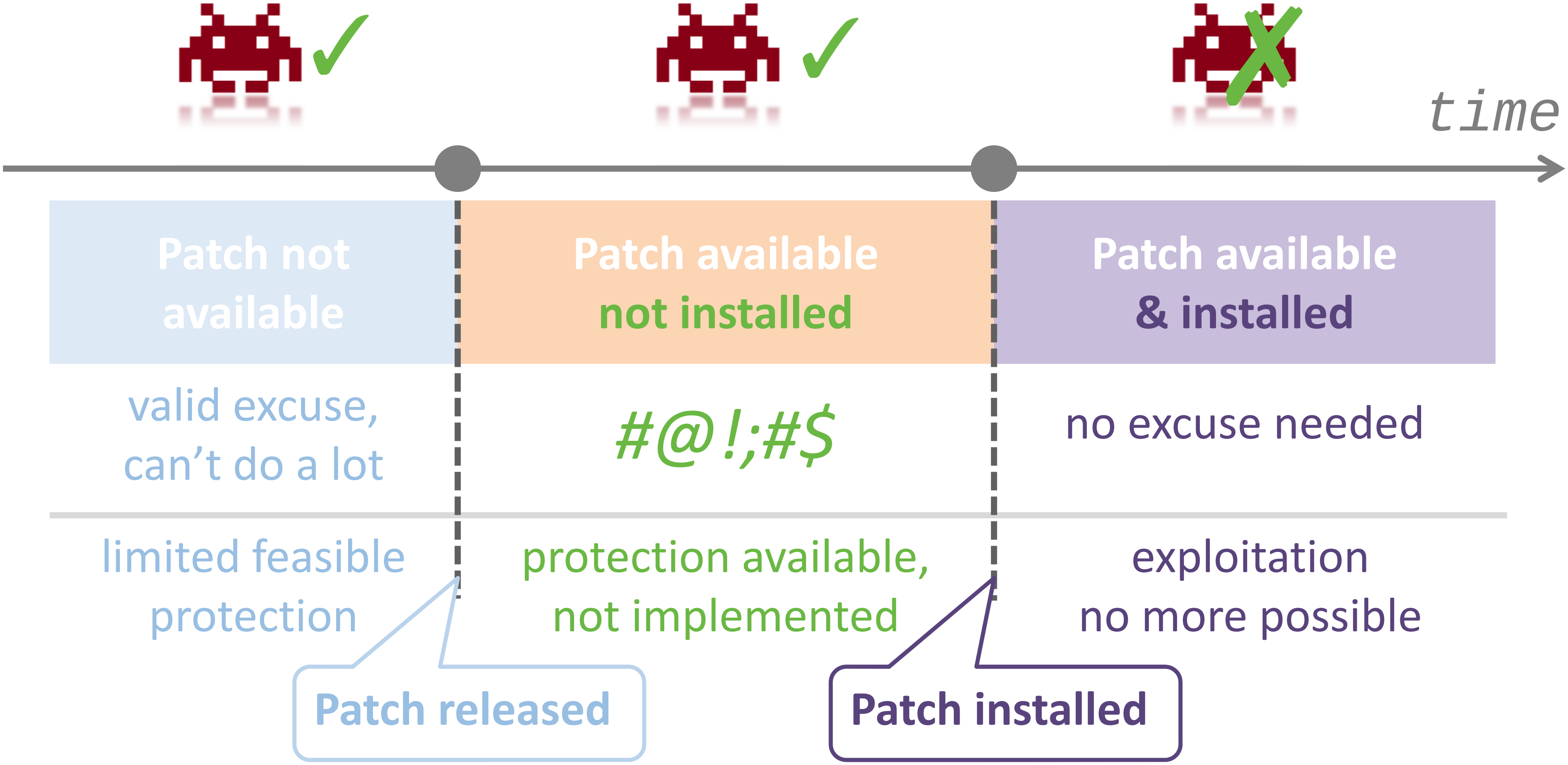
Programs vulnerable in one year, but not in the previous or following year

39%

of the programs vulnerable in one year are not vulnerable in the next year or vice versa

Job Security ..

It depends when you get 0wned



Patch not available	Patch available not installed	Patch available & installed
valid excuse, can’t do a lot	*#@!;#$*	no excuse needed
limited feasible protection	protection available, not implemented	exploitation no more possible

Patch released

Patch installed

A patch provides

better protection

than thousands of signatures

it eliminates the

root cause

Properties of a Patch
.. from a risk & operations perspective

- No false positives (no false alarms)
- No false negatives (no missed attacks)
- No latency or other delays introduced
- No resources whatsoever consumed after deployment

An patch installed essentially terminates the arms race with cybercriminals

The Known Unknowns

Business View

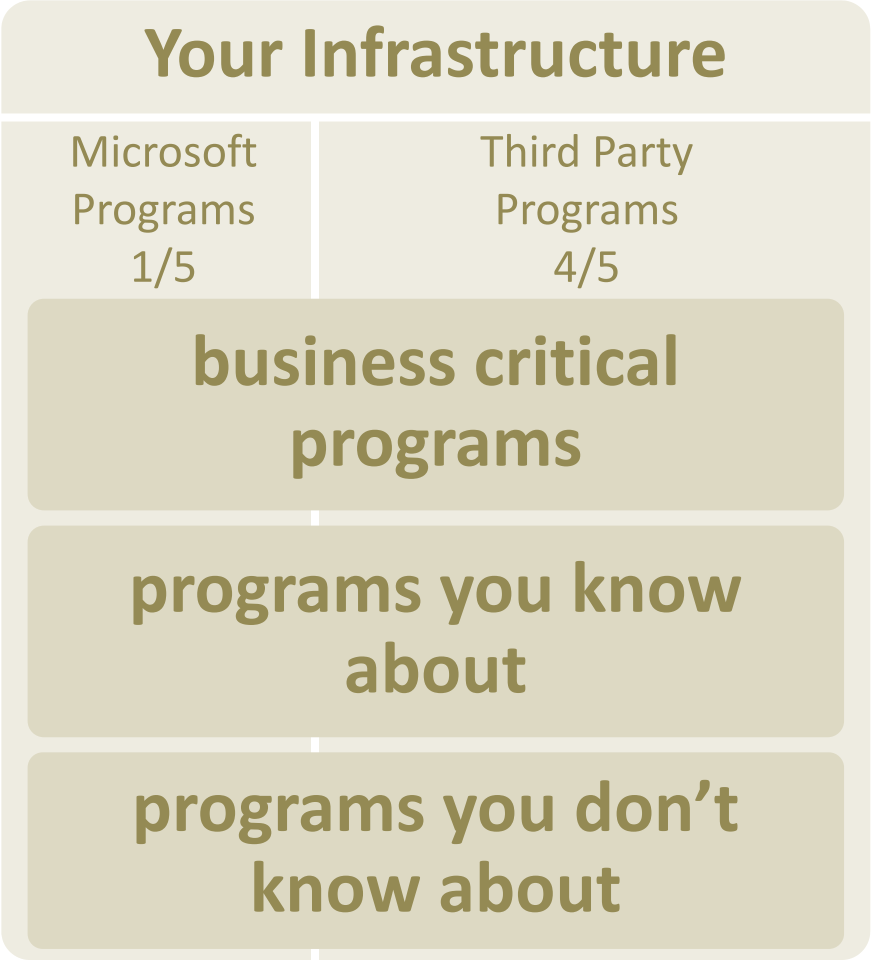
Criminals View

Your Infrastructure	
Microsoft Programs 1/5	Third Party Programs 4/5

The Known Unknowns

Business View

Criminals View



Your Infrastructure

Microsoft Programs 1/5

Third Party Programs 4/5

business critical programs

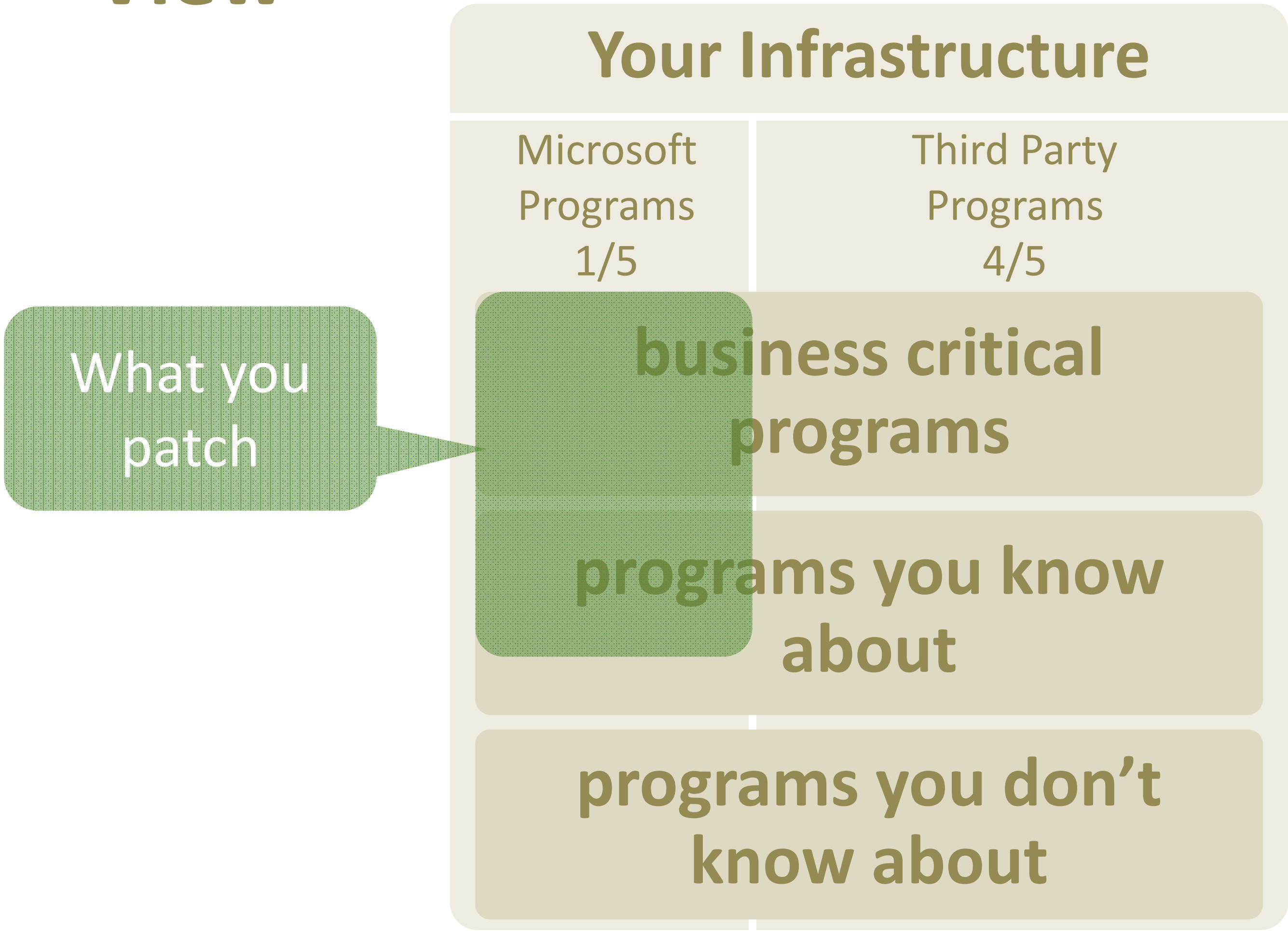
programs you know about

programs you don’t know about

The Known Unknowns

Business View

Criminals View



Your Infrastructure

Microsoft Programs 1/5

Third Party Programs 4/5

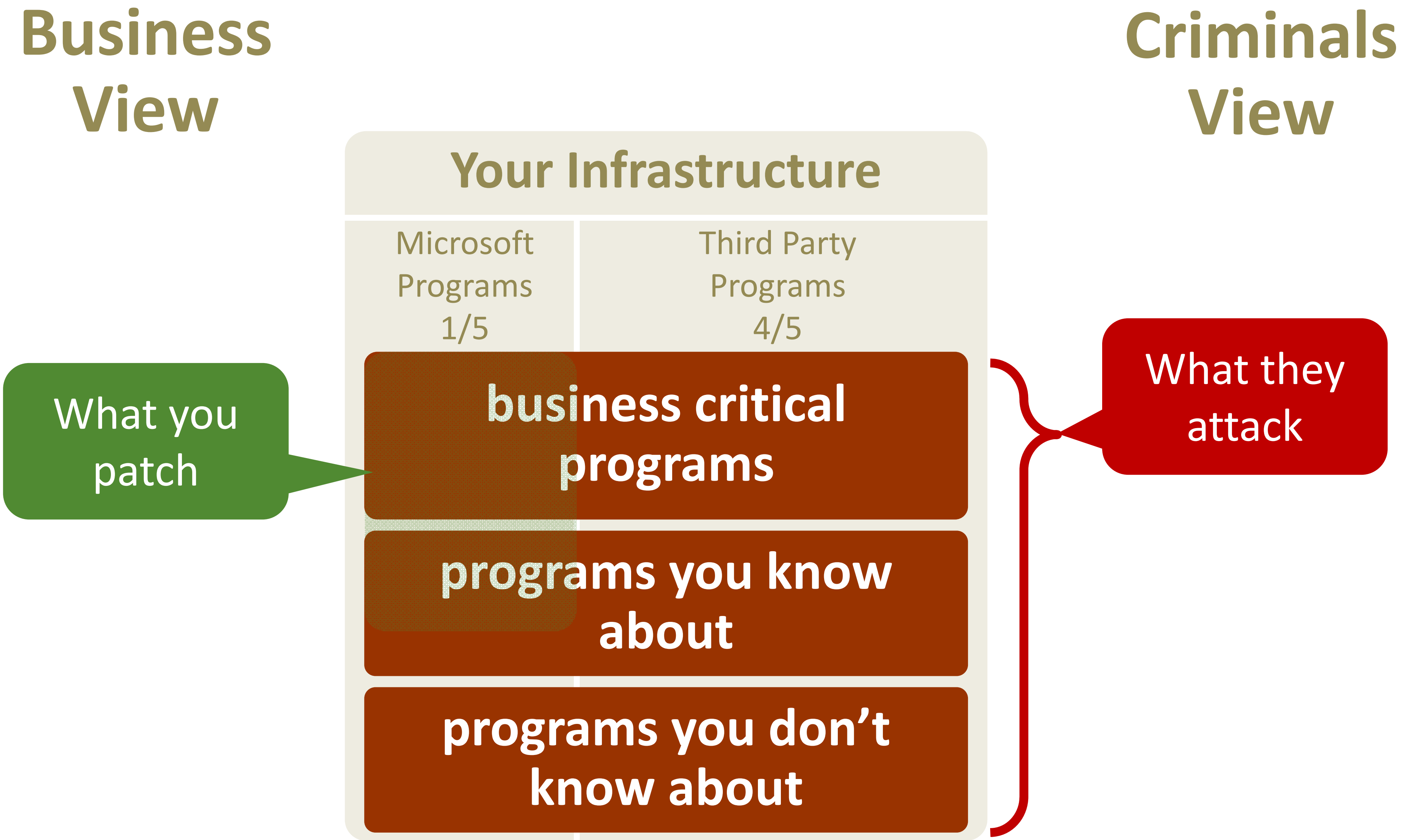
business critical programs

programs you know about

programs you don't know about

What you patch

The Known Unknowns



Business View

Criminals View

Your Infrastructure

Microsoft Programs 1/5

Third Party Programs 4/5

business critical programs

programs you know about

programs you don't know about

What you patch

What they attack

Common Fallacy

Business

Program *X* is not business critical, therefore we won’t spend time patching it

Cybercriminal

Program *X* is just the attack vector to compromise the entire system

X = { Adobe Flash, Reader, Firefox, Java, .. }

Exploitation of any program can compromise the entire end-point

Failure of End-Point Security

What is needed:

- **Reduce Complexity**
  We need tools to simplify and automate patch management in order to master the complexity

- **Intelligence**
  We need tools to enumerate and identify all critical programs to ensure we spend resources on the relevant parts

Conclusion - I

Know your enemy and risks

- **Microsoft is still perceived as the primary attack vector**
  Our defense likely locks the front door while the back door remains wide open

- **Intelligence**
  Knowing all programs and the risks is critical in this dynamic environment
  This saves resources in remediation process

Conclusion - II

Know your tools

- **We need Antivirus, IDS/IPS, ..**
  But we also need to know the limitations of those technologies

- **Patching is a primary security measure**
  Given the effectiveness of eliminating the root cause, and the availability of patches

Stay Secure!

Dr. Stefan Frei

Mail: sfrei@secunia.com
Twitter: @stefan_frei

Supporting Material

- Secunia 2011 Yearly Report
  http://secunia.com/company/2011_yearly_report/
- How to Secure a Moving Target with Limited Resources
  http://bit.ly/hzzlPi
- RSA Paper “Security Exposure of Software Portfolios”
  http://bit.ly/eQbwus
- Secunia Quarterly Security Factsheets
  http://secunia.com/factsheets
- Secunia Personal Software Inspector (PSI)
  free for personal use
  http://secunia.com/psi