Secunia
Stay Secure

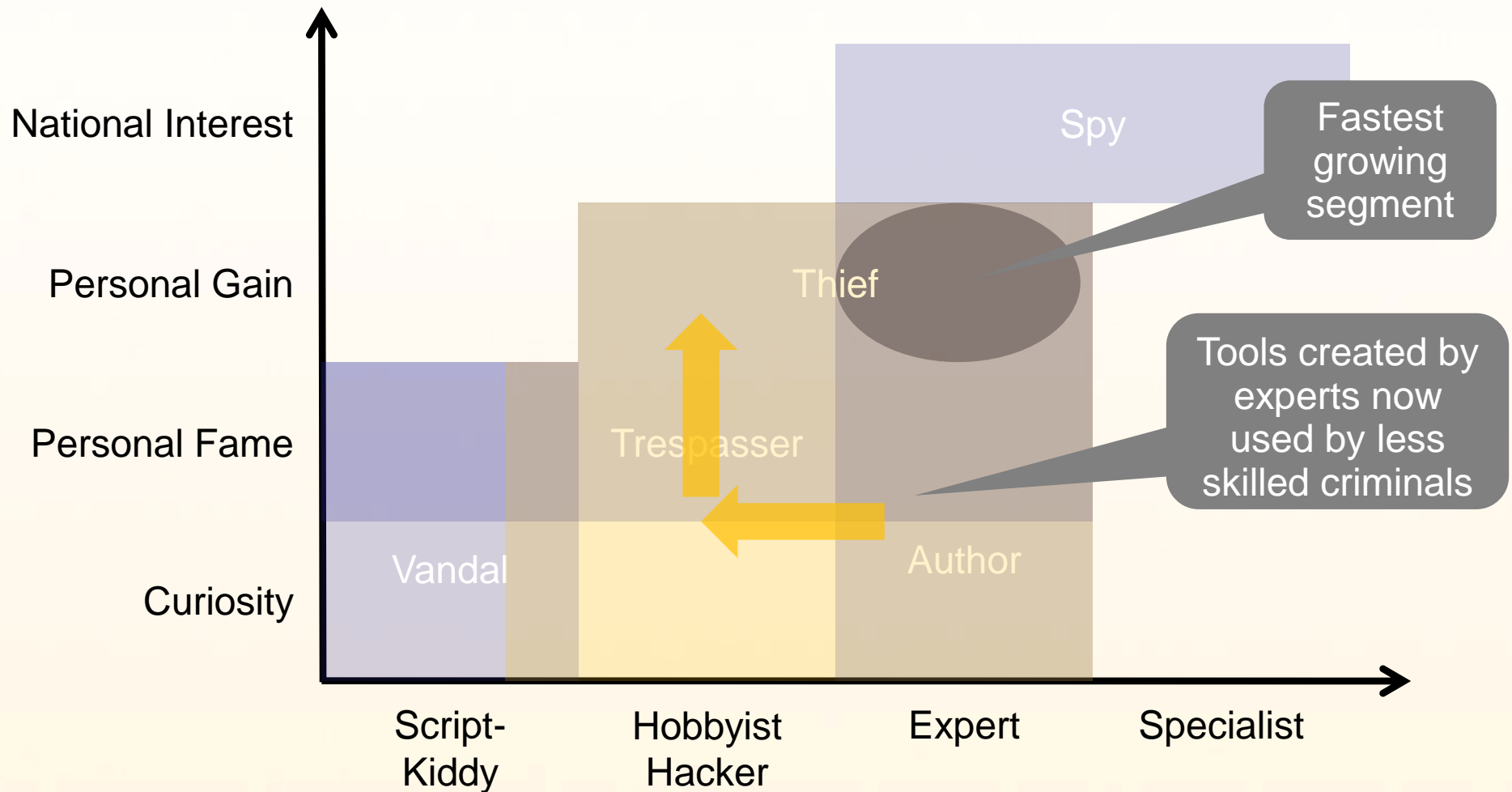# Cybercriminals do not need to target Microsoft

Stefan Frei
Research Analyst Director
sfrei@secunia.com

Agenda

The Changing Threat Environment

National Interest

Personal Gain

Personal Fame

Curiosity

Spy

Thief

Trespasser

Vandal

Author

Script-Kiddy

Hobbyist Hacker

Expert

Specialist

Fastest growing segment

Tools created by experts now used by less skilled criminals

Source: *David Aucsmith, Microsoft*

Today's Cybercrime Landscape

‣ Cybercrime – it is all about profit (+ politics)

‣ Tools created by the experts are used by less skilled attackers
  ‣ more and well armed opportunistic attackers
  ‣ highly automated attacks

‣ Tools are readily available
  ‣ in all shapes and colors
  ‣ or as Malware as a Service (MaaS)

‣ What is the potential of this model?

‣ What are the preferred targets?

Malware & Exploitation Tools

Exploits empowering today's malware - £100 kit

Worm creation kit – turn any executable into a worm

Serial va~~riants~~ ... to fool ar~~ti~~...

Malware ~~antivirus evasion~~ quality te~~sting kit~~

Commercial anti-debugging tools for malware authors

Trojanize legitimate program, spread and stealth

Zeus crimeware platform with plug-in and reporting capability

All offered with a service level agreement and replacement warranty if the tool is detected by any antivirus.

I am not a target

Secunia
Stay Secure

- The "I have nothing to hide" argument:

  - fails short as automated tools do not differentiate

- There is nothing valuable to steal in my infrastructure
  - Well, criminals have plenty of uses for your bandwidth and CPU:

  - hosting malicious content
  - using you as an infection point to spread malware
  - anonymization proxy to hide their activity
  - breaking passwords using your CPU
  - …

Everyone is a valuable target for cybercriminals

World Internet Usage

‣ 6,845 Million World Population and 1,966 Million estimated Internet users on June 30, 2010

World Internet Penetration Rates by Geographic Regions - 2010

Region	Penetration Rate
North America	77.4%
Oceania / Australia	61.3%
Europe	58.4%
Latin America / Caribbean	34.5%
Middle East	29.8%
Asia	21.5%
Africa	10.9%
World, Avg.	28.7%

Penetration Rate (0 – 90%)

- 448% growth of Internet population from 2000 to 2010
- this did not go unnoticed by cybercriminals

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

Secunia
Stay Secure

#Hosts x #Vulnerabilities
=
Opportunity

1,966 Million potential Targets …

‣ End-user PCs are increasingly targeted
    ‣ business PCs as well as personal PCs

‣ End-user PCs is where the **most valuable data** is found the **least protected**

‣ **Eventually**, end-user PCs have **access to all data** needed to **conduct their business**

‣ End-user PCs are commonly exploited..
    ‣ when the user of visits a malicious Web site or opens data, files, or documents ..
    ‣ with one of the numerous programs, or
    ‣ plug-ins installed on his/her PC

What does a typical End-user PC look like?

‣ Highly dynamic environment

‣ Unpredictable usage patterns by users

‣ Numerous programs and plug-in technologies

  ‣ 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?

Secunia
Stay Secure

?

Real Life Data

Under the hood of over 2.6 Mio systems

‣ Secunia Personal Software Inspector (PSI)
  ‣ a free lightweight scanner for Windows PCs
  ‣ scans the users machine for insecure programs
  ‣ installation base > 2.6 million users

‣ Enumerates programs and browser plug-ins installed

‣ Correlation with Secunia's product and vulnerability database **to identify insecure product versions**

‣ Insecure programs:
  ‣ available patches not installed
  ‣ product is end-of-life

‣ Secunia PSI is free for home use
  ‣ http://secunia.com/vulnerability_scanning/personal/

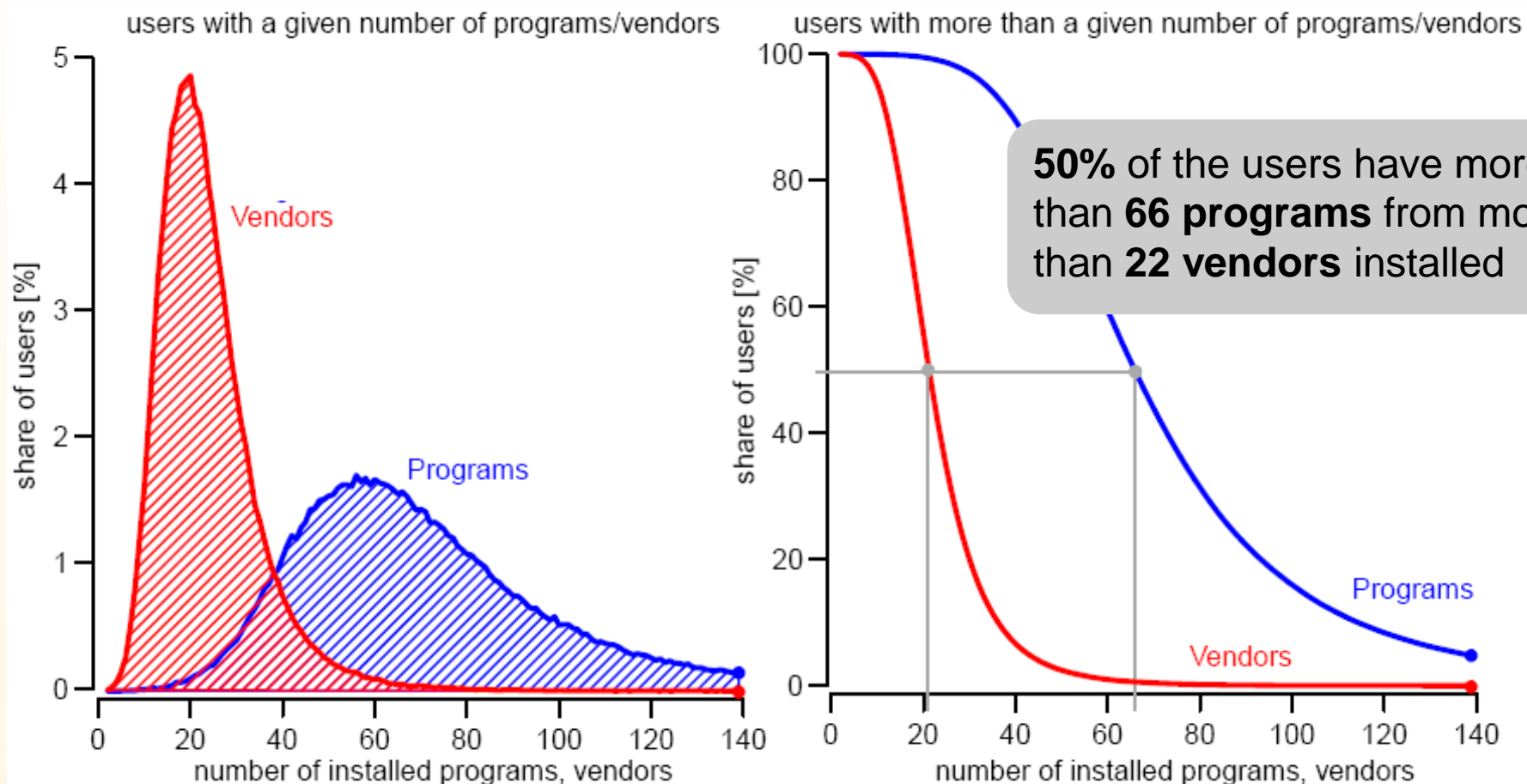# Data Source

Sample Screenshot of PSI

How many products, vendors?

What have users typically installed on their PC

50% of the users have more than **66 programs** from more than **22 vendors** installed

Top-50 software portfolio

Looking at a typical end-user PC

▸ Based on PSI scans we identified the portfolio of the Top-50 most prevalent programs on typical end-user PCs

▸ The Top-50 portfolio consists of
  ▸ 26 Microsoft and
  ▸ 24 non-Microsoft (3rd party) programs
  ▸ from 14 different vendors

▸ Each program in the Top-50 has at least a 24% user-share

▸ Eight programs from three vendors have more than a 80% user-share
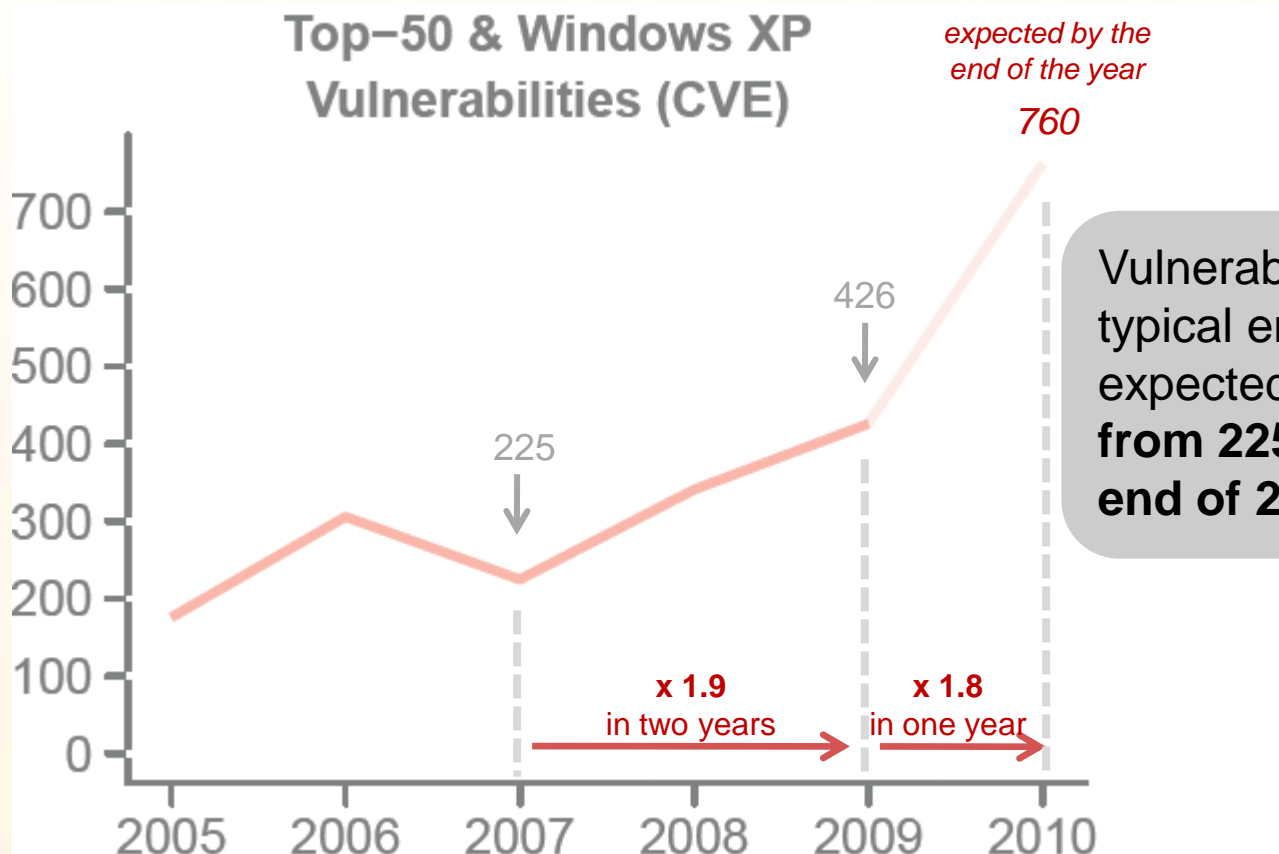
.. and relevant Trend

More than **50%** of these vulnerabilities are rated as **highly** or **extremely** critical, providing **system access** to the victims host

Criticality in % of advisores

Extreme	
High	
Moderate	
Less	
Not	

0% 25% 50% 75% 100%
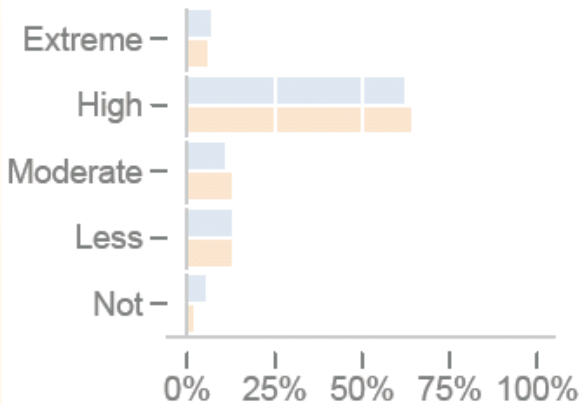
Attack vector in % of advisories

Local system	
From remote	
From local network	

0% 25% 50% 75% 100%

Impact in % of advisores

System access	
Security Bypass	
Privilege escalation	
Exposure of sensitive information	
DoS	

0% 25% 50% 75% 100%
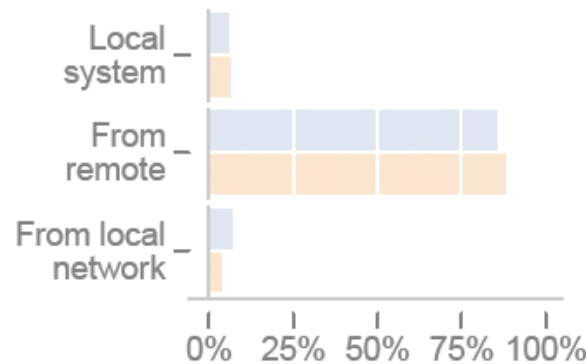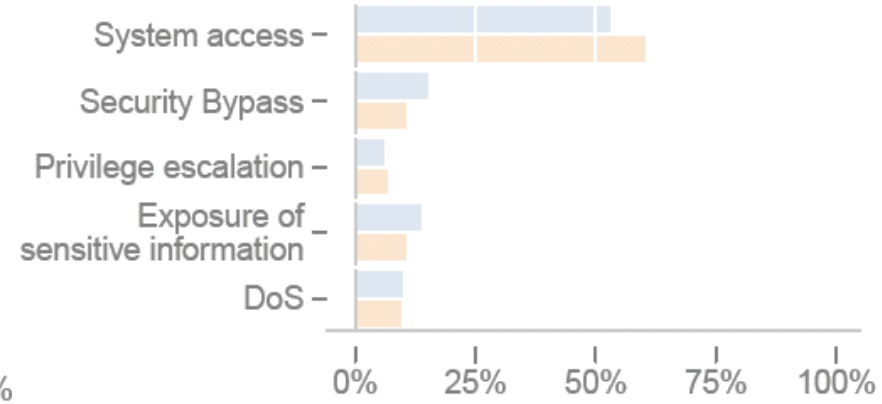
Year-on-year analysis of the last 12 months periods as of 2010-Q3

previous 12 months   current 12 months

2008   2009   2010   2011
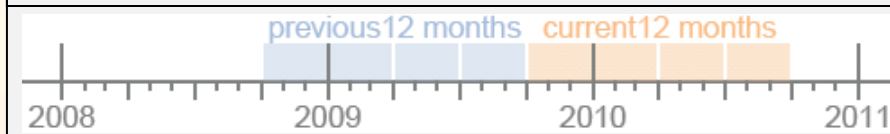
Root Cause Analysis

‣ What are the sources of these vulnerabilities?

‣ Vulnerability contributions by

‣ (A) Operating System

‣ (B) Microsoft Programs

‣ (C) Third-party Programs (non MS)

Root cause analysis

3rd party program vulnerabilities are found
to be almost exclusively responsible for this trend

Top 3rd Party Programs

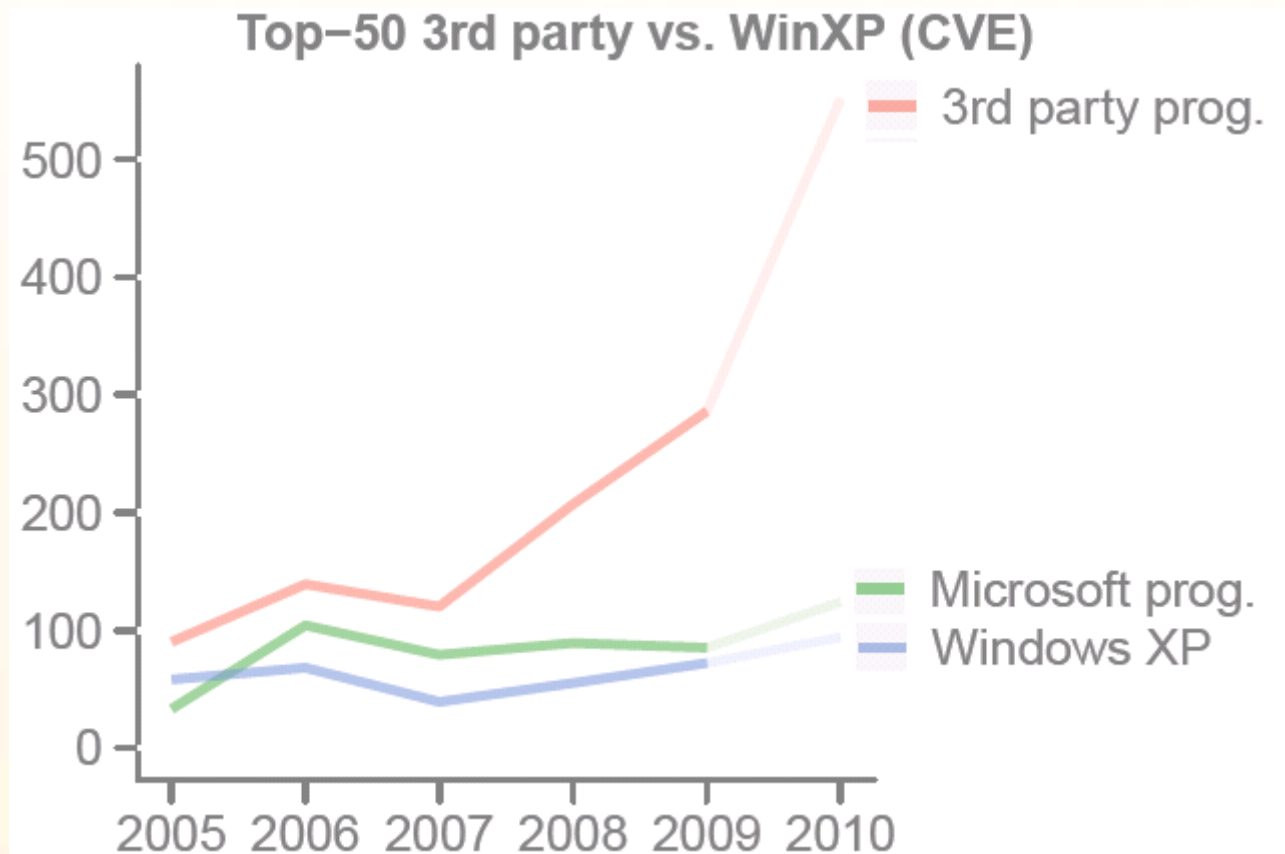| Top-10 3rd Party Programs (ranked by # of vulnerabilities)			June 2009-2010	
Rank Program	Vendor	Installation share	CVEs	Events
1. Mozilla Firefox	Mozilla Foundation	56%	96	15
2. Apple Safari	Apple	15%	84	9
3. Sun Java JRE	Sun (Oracle)	89%	70	5
4. Google Chrome	Google	30%	70	14
5. Adobe Reader	Adobe	91%	69	7
6. Adobe Acrobat	Adobe	8%	69	7
7. Adobe Flash Player	Adobe	99%	51	4
8. Adobe AIR	Adobe	41%	51	4
9. Apple iTunes	Apple	43%	48	3
10. Mozilla Thunderbird	Mozilla Foundation	10%	36	7

Approx. number of actions required to keep
the program secure in 12 months

Top Microsoft Programs

Top-10 Microsoft Programs (ranked by # of vulnerabilities)			June 2009-2010	
Rank Program	Vendor	Installation share	CVEs	Events
1. Internet Explorer	Microsoft	100%	49	12
2. Excel Viewer	Microsoft	2%	37	4
3. Excel	Microsoft	78%	30	5
4. Visual Studio	Microsoft	5%	15	3
5. .NET Framework	Microsoft	95%	13	4
6. Visio Viewer	Microsoft	35%	11	2
7. Visio	Microsoft	3%	11	3
8. Word Viewer	Microsoft	3%	9	2
9. Works	Microsoft	7%	9	2
10.Project	Microsoft	3%	9	2

Approx. number of actions required to keep
the program secure in 12 months

From a Cybercriminals perspective

▸ User's and businesses alike still perceive the operating system and Microsoft products to be the primary attack vector, largely ignoring 3rd party programs

▸ The frequency and complexity of managing a large number of different update mechanisms will almost certainly lead to incomplete patch levels at large

Cybercriminals do not need precious 0-day vulnerabilities

Cybercriminals do not need Microsoft vulnerabilities

▸ **Cybercriminals act based on the harsh reality, instead of conceptualizing on how a perfect(ly) (patched) world is supposed to look like.**

Secunia
Stay Secure

Most common Myth

Once a patch for a particular flaw is available, case is closed

‣ The lack of prioritization of the second stage in the process, **patch installation**, results in the current situation where one of the world's largest botnets, Conficker, continues adding new hosts

‣ Numerous users don't have a clue that they're getting themselves infected through flaws which have been patched by the vendor long ago

‣ Exploit availability skyrockets upon patch release
    ‣ Cybercriminals are good at reverse engineering patches

What does all this mean?

▸ From a criminals perspective, targeting 3rd party programs proves to be a rewarding path, and will remain so for an extended period of time.

▸ In the Top-50 portfolio in 2009
  - ▸ 3rd party programs had 286 vulnerabilities,
  - ▸ 3.5x more than the Microsoft programs

▸ In the Top-50 portfolio in 2010 (first half year)
  - ▸ 3rd party programs had 275 vulnerabilities,
  - ▸ 4.4x more than the Microsoft programs

▸ Only one exploitable vulnerability is needed to compromise the PC.

What do we do today?

Updating the typical end-user PC

▸ To keep a PC with the top 50 portfolio fully patched, the user has to master **14 different** update mechanisms:

▸ **One** update mechanism ..
  ▸ to patch **the OS and the 26 Microsoft programs**
  ▸ to cover **35%** of vulnerabilities

▸ Another **13 different** update mechanisms ..
  ▸ to patch the remaining **24 3rd party programs**
  ▸ to cover **65%** of vulnerabilities

▸ Thus, 3rd party programs are unlikely to be found fully patched on a PC.

Do you manually update antivirus signatures?

Do you manually run backups?

How do you enumerate and patch 3rd party programs?

BINGO

[shuffle]
68511

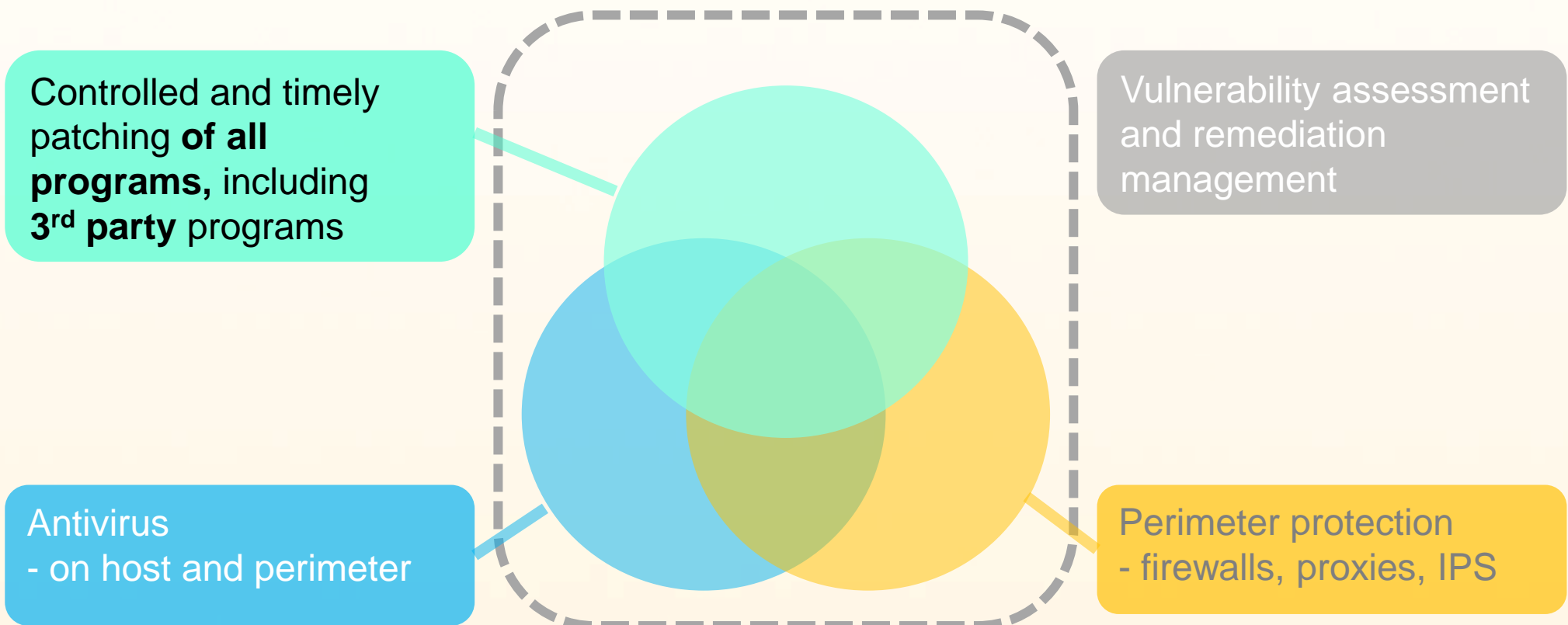|				
NO ONE HAS EVER FOUND ANY PROBLEMS	WE THINK IT IS SECURE ENOUGH	WE DON'T COMMENT ON SECURITY MATTERS	IT WOULD BE TOO EXPENSIVE TO FIX THAT	YOU'RE JUST LOOKING FOR ATTENTION
IT'S A FEATURE OUR USERS WANT	WE MEET ALL GOVERNMENT STANDARDS	YOU'RE SO NEGATIVE	OUR PROACTIVE TECHNOLOGY SOLUTIONS PREVENT THAT	WHAT DO YOU HAVE AGAINST US?
WE MEET ALL INDUSTRY STANDARDS	YOU MUST BE BEING PAID BY OUR COMPETITION	SECURITY PROBLEM EXCUSE BINGO	THE PRODUCT WAS TESTED BY SECURITY EXPERTS	WE HAVE CISSP CERTIFIED ENGINEERS
NO ONE WOULD EVER THINK OF THAT	THE ANTI-VIRUS SOFTWARE DID IT	WHO ARE YOU TO CRITICIZE, ANYWAY?	WHY ARE YOU TRYING TO HARM OUR INDUSTRY?	IT DOESN'T NEED TO BE VERY SECURE
YOU ARE IN VIOLATION OF THE DMCA	NOBODY'S PERFECT	YOU'RE JUST AN ACADEMIC	NO COMMENT	WE ALREADY KNEW ABOUT IT
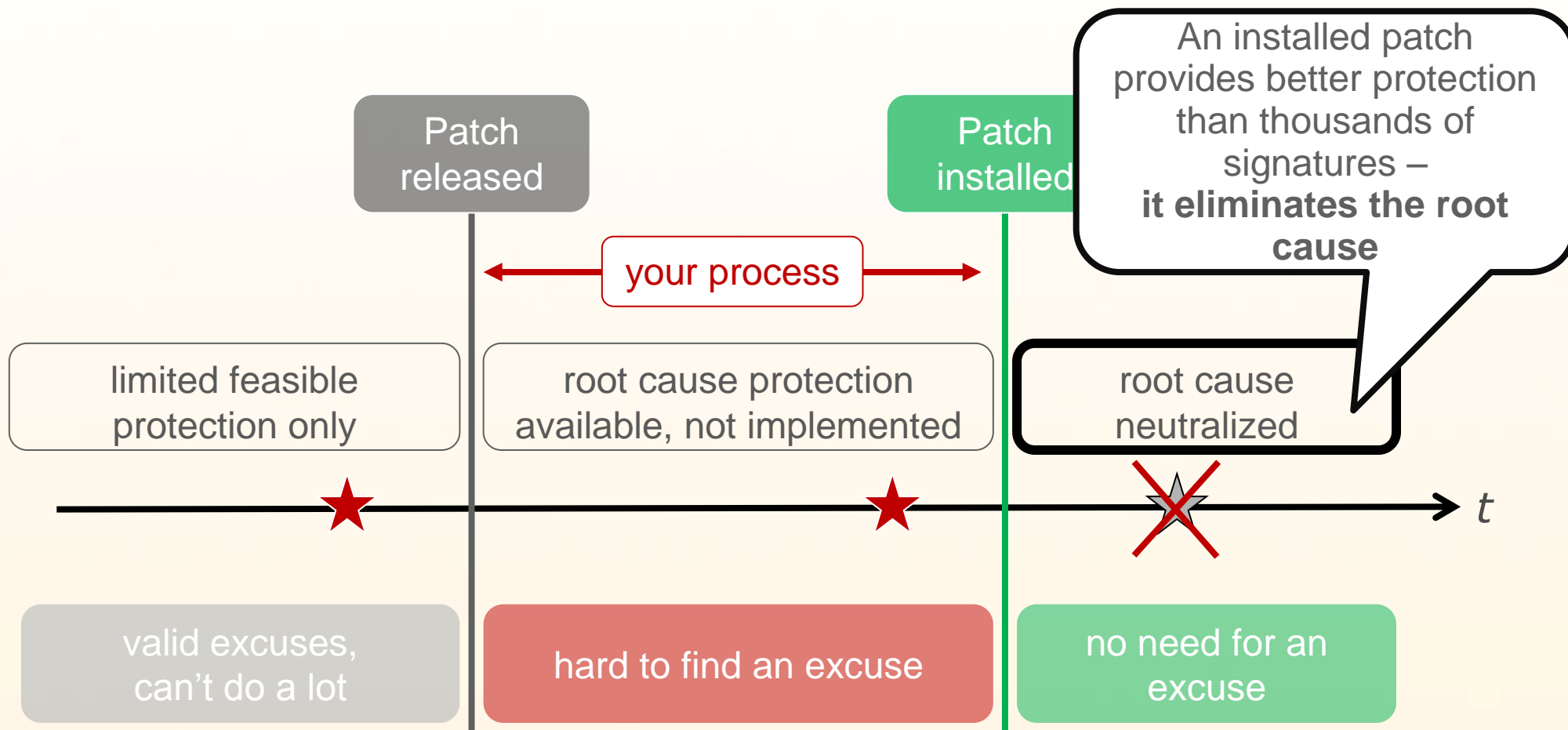
Multi Layer Defense

- there is no single silver bullet technology
- systematically know where you are vulnerable
- control the remediation process

Controlled and timely patching **of all programs,** including **3rd party** programs

Vulnerability assessment and remediation management

Antivirus
- on host and perimeter

Perimeter protection
- firewalls, proxies, IPS

Conclusion

‣ User's and businesses alike still **perceive** the operating system and Microsoft products to be the primary attack vector, largely **ignoring 3rd party** programs

   ‣ locking the front door while the backdoor remains widely open

‣ Patching is still seen as **secondary measure** compared to anti-virus and perimeter protection

‣ **Controlled** and **timely** patching of **all programs** is needed

Stay Secure!

Supporting Material

‣ Secunia 2010 half year report
on the threat of 3rd party programs

http://secunia.com/gfx/pdf/Secunia_Half_Year_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/blog/123

‣ Secunia Corporate Software Inspector (CSI)
http://secunia.com/vulnerability_scanning/corporate