




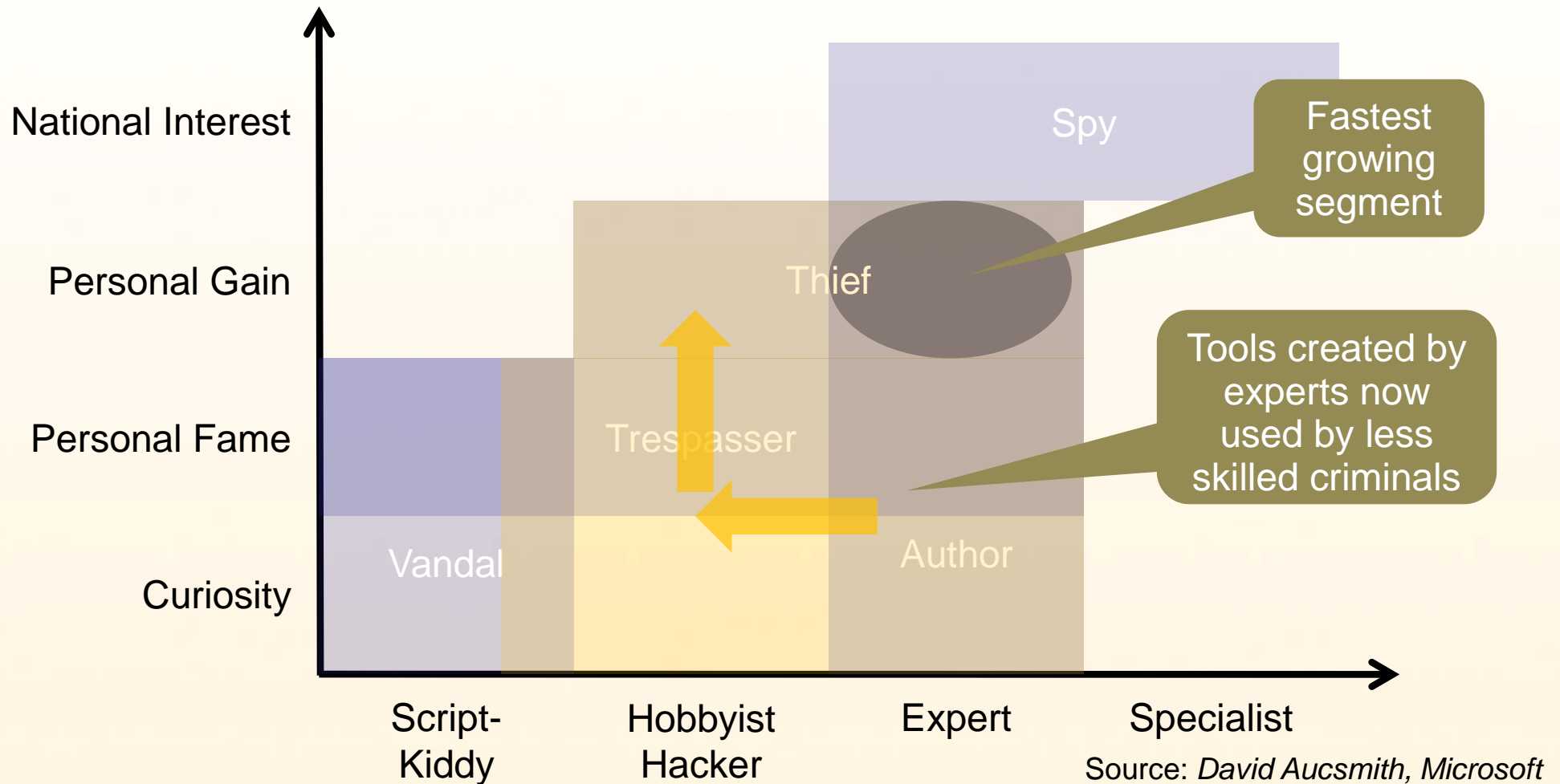
# The Fundamental Failures of End-Point Security

Stefan Frei  
Research Analyst Director  
[sfrei@secunia.com](mailto:sfrei@secunia.com)

# Agenda

- 
- ▶ The Changing Threat Environment
  - ▶ Malware Tools & Services
  - ▶ Why Cybercriminals Need No 0-Days
  - ▶ Complexity of Patching
  - ▶ Defense Strategies

# The Changing Threat Environment



# 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 Ecosystem

- ▶ Malware Creation
  - ▶ Cybercriminals use a broad **spectrum of tools** and techniques to create **one-of-a-kind packages** that easily **bypass** traditional antivirus technologies
- ▶ Cyber-criminal can selectively apply manipulation technologies to their creations that **radically alter the fabric** of malware
- ▶ Result: **Stealthy Threats**
  - ▶ that evade signature-based detection systems, static analysis tools, behavioral monitoring environments and sandbox technologies

# Serial Variants & Permutations

- ▶ Tactics
  - ▶ **Multiple variants** of a particular malware agent are created **in advance** of the attack
  - ▶ Each new variant is released at scheduled intervals to constantly **remain ahead** of antivirus protection updates
- ▶ Process
  - ▶ Automatically create 10'000 variants of your malware and release a first batch of 1,000 samples
  - ▶ As soon as the first batch is detected by antivirus, release the next 1,000 samples ...
  - ▶ Result: antivirus is playing catch-up

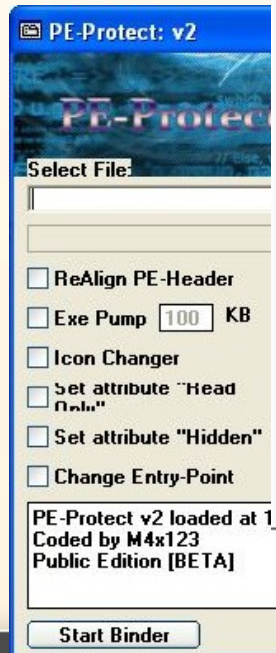
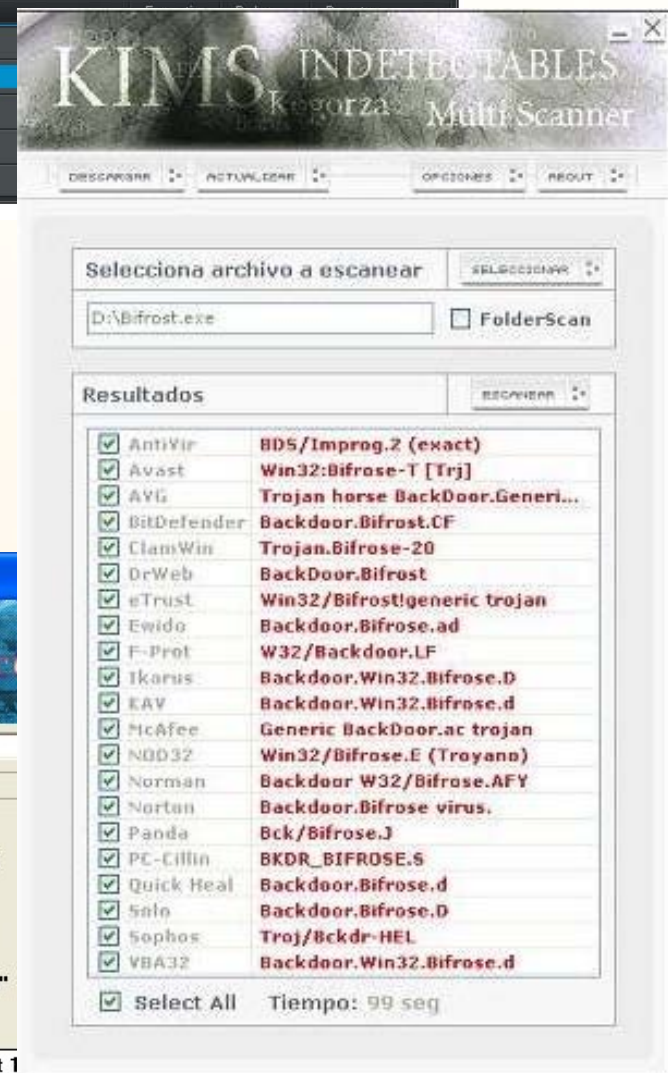
# Tools of the Trade

- ▶ Cryptor
  - ▶ **encrypt malware** so that signature detection systems and static analysis processes are ineffectual
- ▶ Protector
  - ▶ **add anti-debugging features** that thwart security researchers and automated sandbox analysis technologies




# Tools of the Trade

- ▶ Binder
  - ▶ “embed” malware and trojanize other software packages
  - ▶ aiding propagation of malware, **tricking victims** into executing something **that looks legitimate**
- ▶ Quality Assurance
  - ▶ Malware is passed through multiple antivirus products to verify it will **not be detected prior** to their criminal deployment




# Malware Ecosystem & Services



**Silver Edition**

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/Vista
- Webcam streaming is available with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies chngements on clipboard and save them

Price : 179\$ (United State Dollar)



**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 chngements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249\$ (United State Dollar)

- ▶ Malware automatically cycles through a **large number of exploits** until one succeeds to compromise the target
- ▶ Systematic and **automated** exploitation of victims at large scale
- ▶ The tools are readily available, no expertise needed

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

# I am not a target

- ▶ 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

$$\begin{aligned} \# \text{Hosts} \times \# \text{Vulnerabilities} \\ = \\ \text{Opportunity} \end{aligned}$$

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

## World Internet Usage

# 1,966 Million

estimated Internet users on June 30, 2010

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

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

# 1,966 Million potential Targets ...

- ▶ **Business** as well as **personal end-point PCs** are increasingly targeted
- ▶ End-point PCs is where the **most valuable data** is found the **least protected**
- ▶ Eventually, end-point PCs have access to all data needed to conduct their business

## Some Real Life Stats Botnet Infections in Enterprises

- ▶ Up to **9 percent** of the end-point PCs in enterprises are found infected
- ▶ Of all enterprises looked at, **100 percent** had bot infections
- ▶ **Best of breed** antivirus, perimeter protection, and IDS/IPS do not provide 100% detection

Source: Darkreading <http://bit.ly/EntBot>

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

## What does a typical End-point 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?

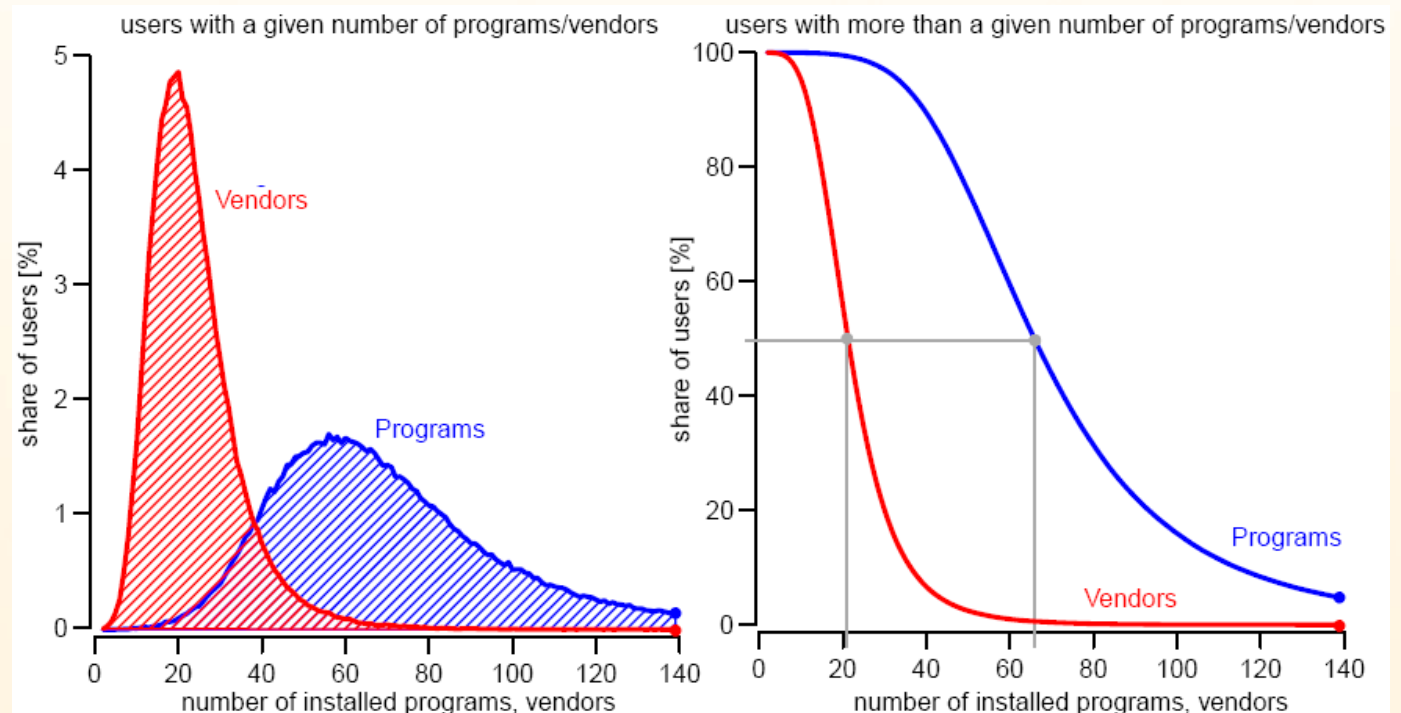


# A typical end-point PC software portfolio

- ▶ Secunia Personal Software Inspector (PSI)
  - ▶ A lightweight scanner for Windows PCs to identify **insecure programs** and **plug-ins**
  - ▶ Secunia PSI is free for home use
  - ▶ Insight from data of more than 3 Mio end-point PCs
- ▶ A program version is considered insecure if
  - ▶ .. available **patches are not installed**
  - ▶ .. the product is **end-of-life**

What have users typically installed on their end-point PC?

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



- ▶ The **Top-50 software portfolio** contains the 50 most prevalent programs to represent a typical endpoint PC
  - ▶ each program in the Top-50 portfolio has at least a 24% user-share, eight programs from three vendors have more than a 80% user-share



- ▶ The Top-50 portfolio consists of **26 Microsoft** and **24 third party** (non-Microsoft) programs from **14 different vendors**

# Top-10 by vulnerabilities

**Top-10 3rd Party Programs** (ranked by # of vulnerabilities)

Rank Program	Vendor	Installation share	June 2009-2010	
			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

**Events**

Approx. number of administrative events to keep program secure in 12 months

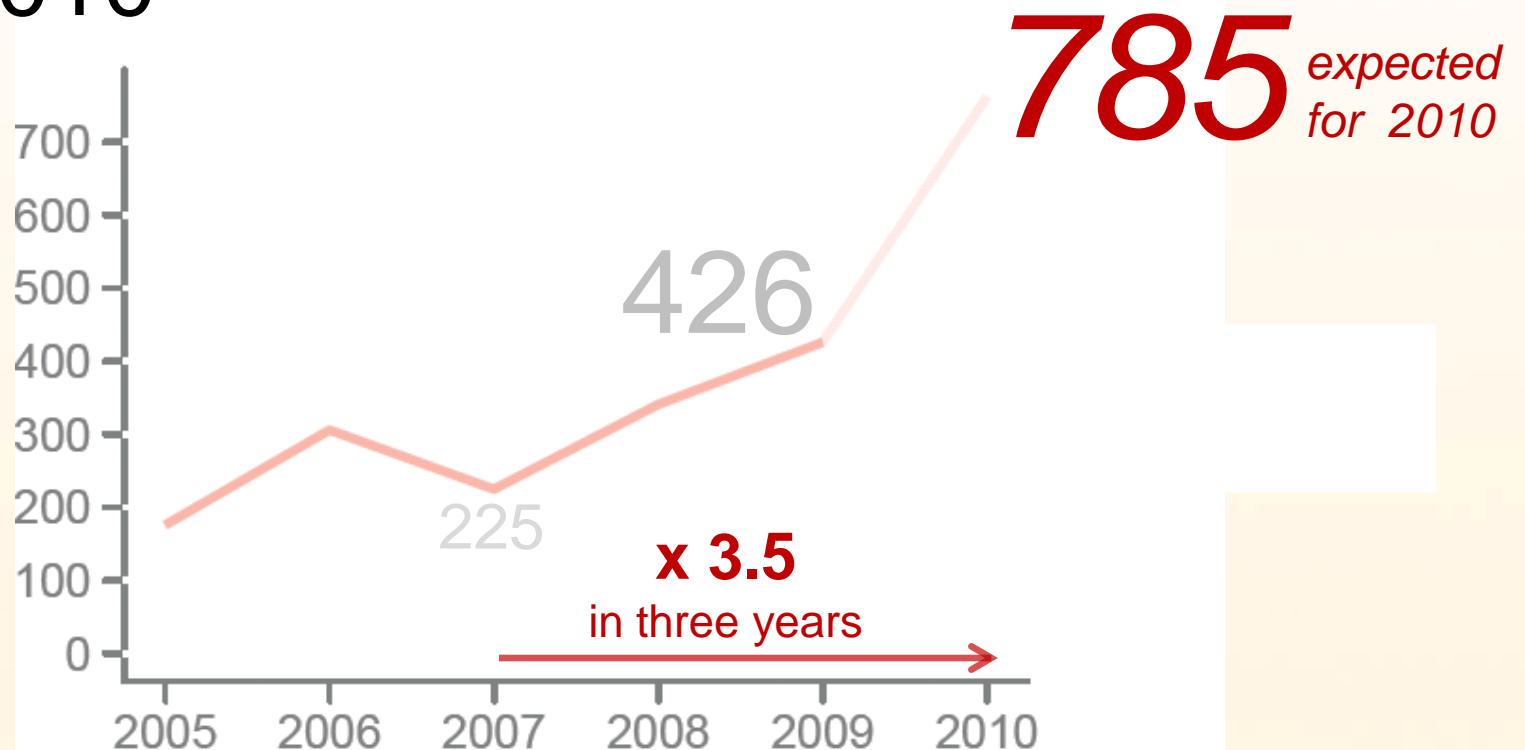
**CVEs**

Number of vulnerabilities in 12 months

**Top-10 Microsoft Programs** (ranked by # of vulnerabilities)

Rank Program	Vendor	Installation share	June 2009-2010	
			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

**Vulnerabilities** affecting a typical end point increased **3.5 times** to 785 per year from 2007 to 2010



## A relevant Trend ..

more than

**50 percent** of these vulnerabilities  
are rated as **highly** or **extremely** critical

.. providing **system access** to  
the victims of exploitation

# What are the major contributors of this increasing trend?

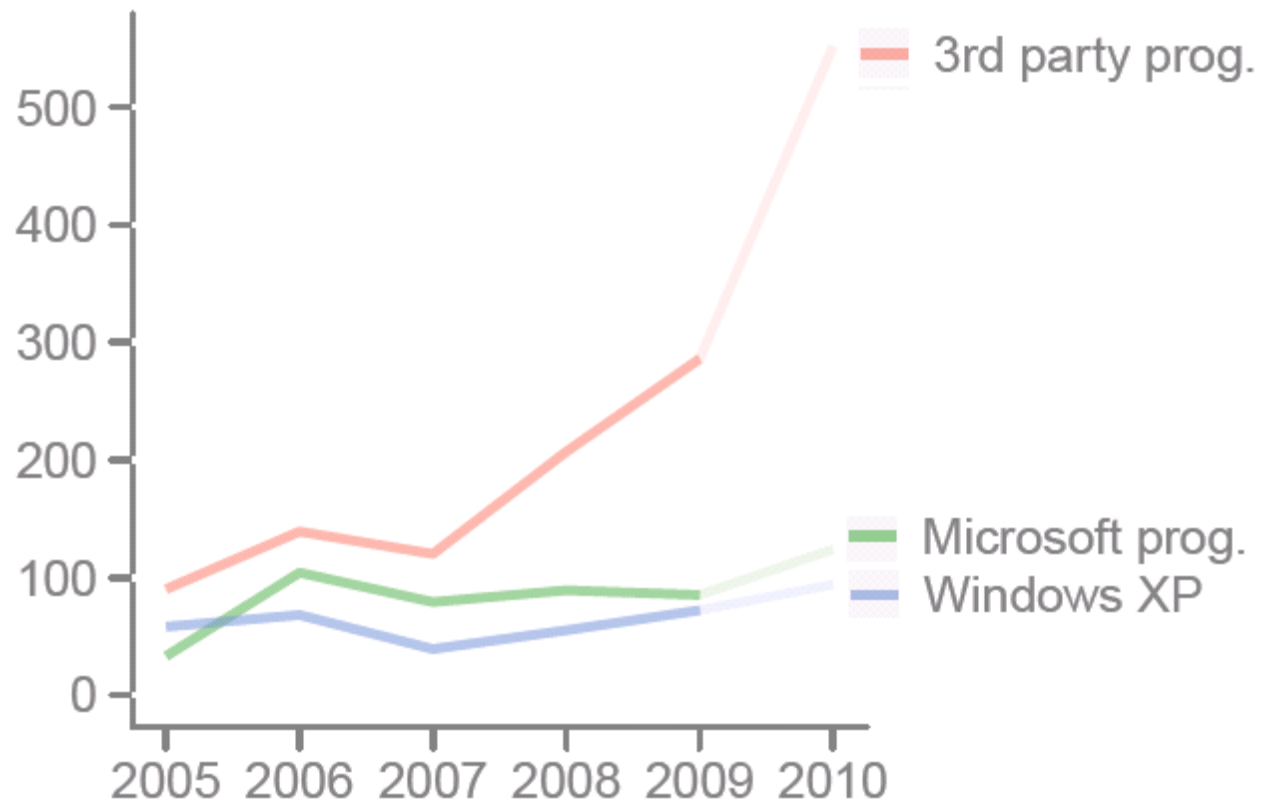
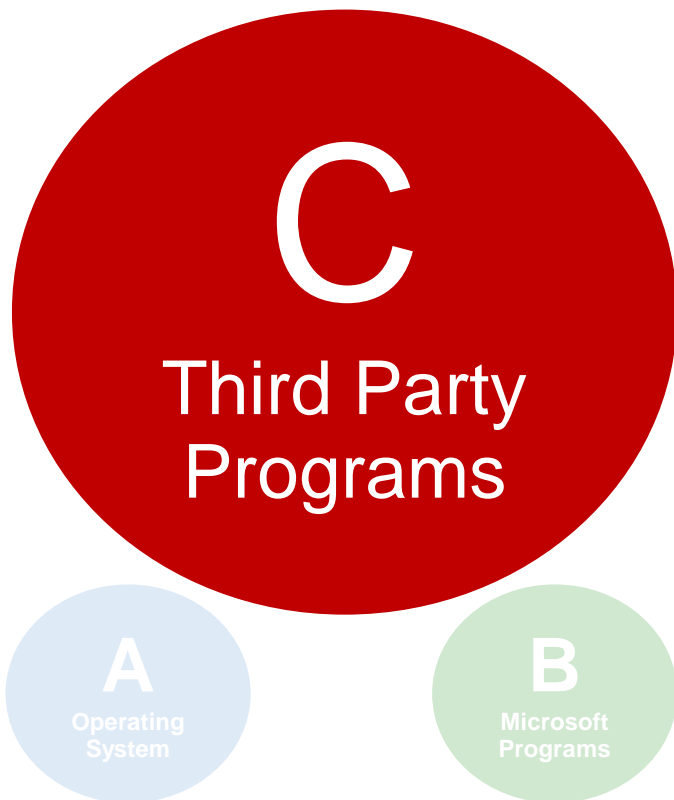


**A**  
Operating System

**B**  
Microsoft Programs

**C**  
Third party Programs

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



## Updating the typical end-point PC

- ▶ To keep a PC with the Top 25 vulnerabilities patched, the user has to manage a total of **14 different** update mechanisms:

Do you manually update antivirus signatures?

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

Do you manually run backups?

- ▶ Another **13 different** update mechanisms...
  - ▶ to patch the remaining **24 third party** programs
  - ▶ to cover **65%** of vulnerabilities

How do you enumerate and patch 3<sup>rd</sup> party programs?

## Current State

- ▶ User's and businesses alike still **perceive** the operating system and Microsoft products to be the primary attack vector, **largely ignoring third 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

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

Cybercriminals act based on the harsh reality, which is that **numerous unpatched programs are present at any time.**

They don't need to conceptualize on how a perfectly patched world is supposed to look like.

## From a Cybercriminals perspective

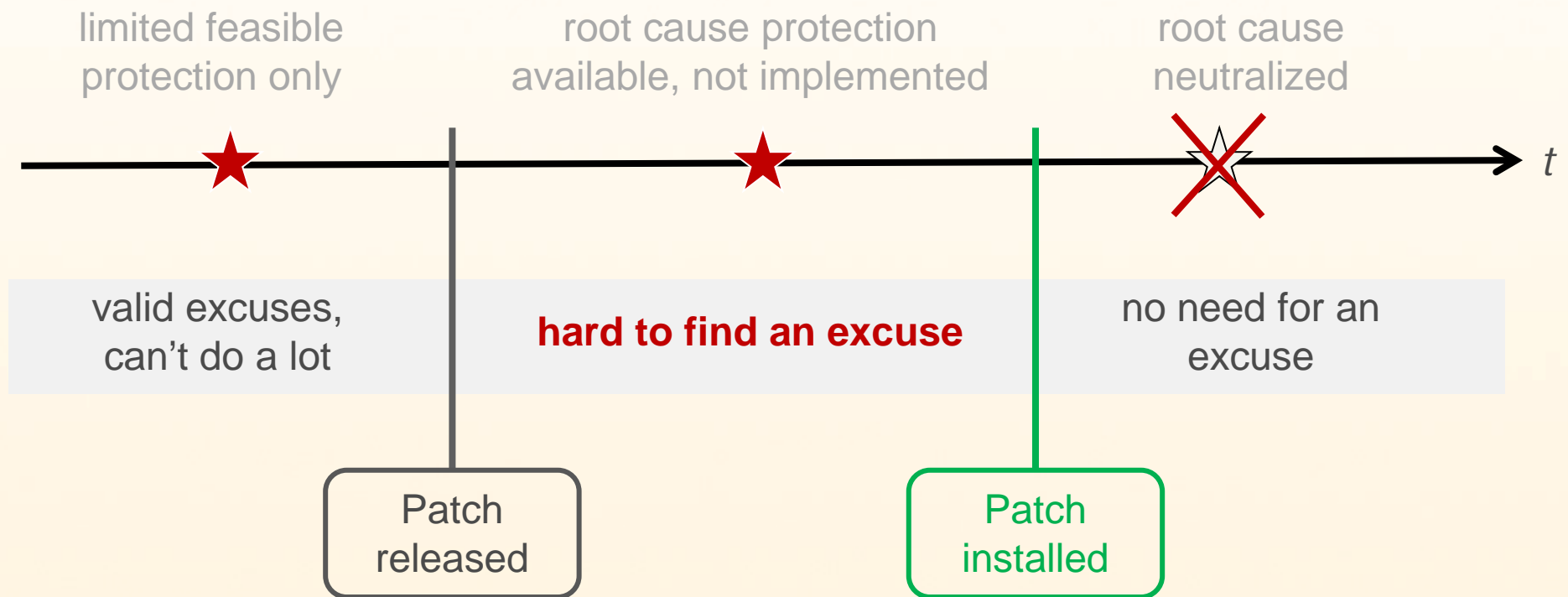
- ▶ Targeting third party programs proves to be a rewarding path, and will remain so for an extended period of time.
- ▶ In the Top-50 portfolio in 2009
  - ▶ Third party programs had **286** vulnerabilities,
  - ▶ **3.5x more** than the Microsoft programs
- ▶ In the Top-50 portfolio in 2010 (first half year)
  - ▶ Third party programs had **275** vulnerabilities,
  - ▶ **4.4x more** than the Microsoft programs
- ▶ Only **one exploitable vulnerability** is needed to compromise an end-point PC.

# Updating the typical end-point PC

- ▶ How to manage 150 patches for 50 programs of 14 different vendors per year?
- ▶ Any manual approach is doomed to fail and will leave many programs **unpatched for extended** periods
  - ▶ Easy prey for cybercriminals
- ▶ Process Requirements
  - ▶ automatically identify **all third party** programs
  - ▶ verify the **patch level** of the programs found
  - ▶ report **missing patches** or **insecure** installations
  - ▶ **install** the missing patches

# Responsibility

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



A patch provides  
better protection  
than thousands of signatures

it eliminates the  
root cause

# 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 **third 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 third 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 **identification** and **timely patching** of all programs, incl. third party programs, is needed

# Personal Software Inspector PSI 2.0 Beta

- ▶ Free auto-update for third party programs
- ▶ Automatically **updates** a growing number of frequently used 3<sup>rd</sup> party programs
  - ▶ (i.e. Adobe Reader, Flash Player, Firefox, Java, Skype, ..)
- ▶ Choose “one click” or silent update mode
- ▶ First results: PSI 2.0 **patches many programs** that come with **their own update mechanism!**
- ▶ Secunia PSI 2.0 uses the same framework and engine which is used in our robust commercial solution, the Corporate Software Inspector (CSI)



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](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](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](http://secunia.com/vulnerability_scanning/corporate)