Secunia

Stay Secure

The Fundamental Failures of End-Point Security

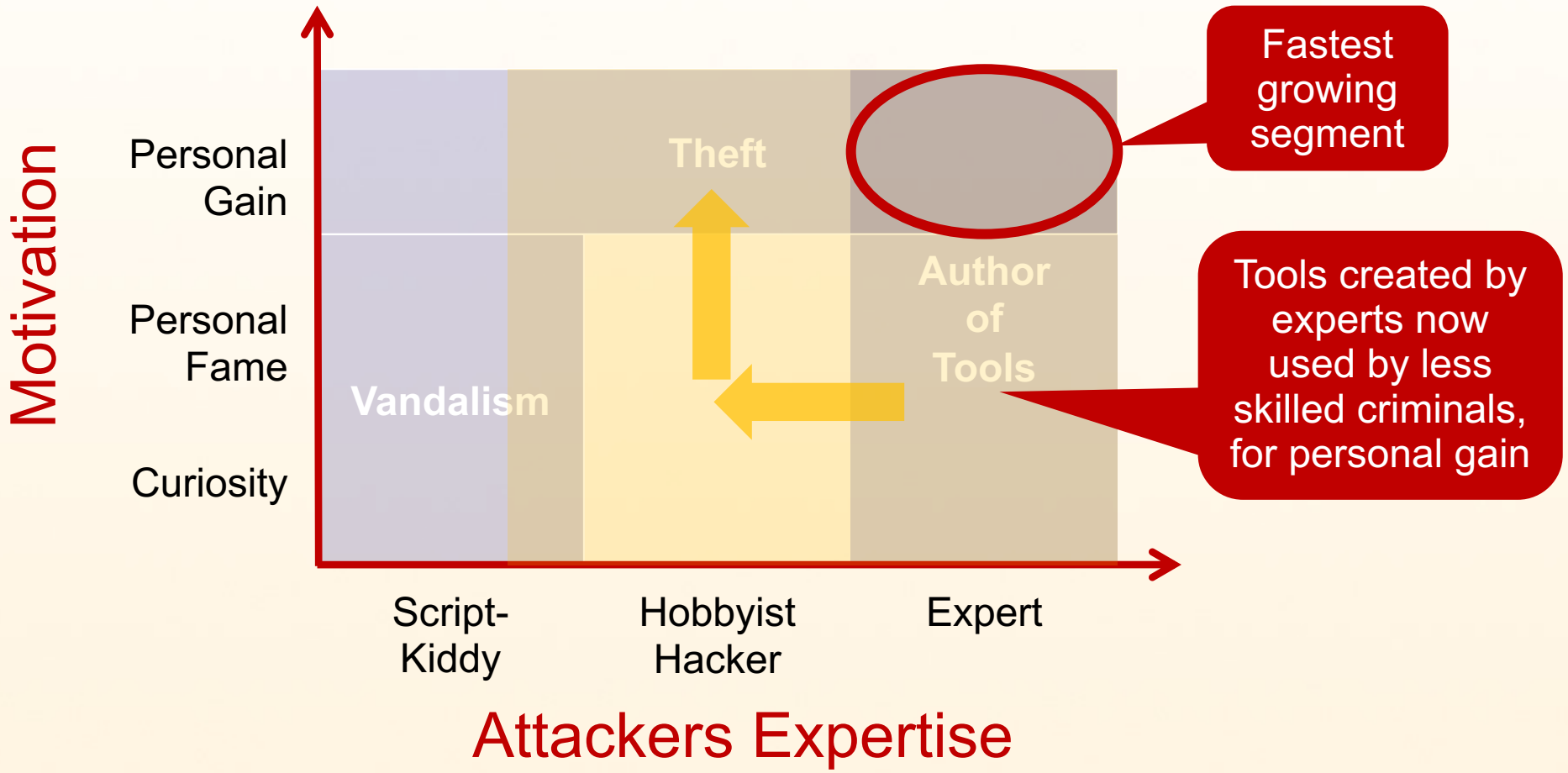
Dr. Stefan Frei
Research Analyst Director

sfrei@secunia.com

Agenda

- The Changing Threat Environment
- The Software Portfolio of a Typical End-Point PC
- An Alarming Trend
- Complexity of Patching

The Changing Threat Environment



Cybercrime – it's all about Profits

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

World Wide Internet Usage

1,966 Million

estimated Internet users on 31st December, 2010

28% penetration of population

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-points are increasingly targeted
- End-point PCs are where the most valuable data is found to be the least protected
  - Eventually end-point PCs have access to all data needed to conduct their business
- But I am not a primary target ...
  - fails short as automated tools do not differentiate

Everyone is a valuable target for cybercriminals

End-Points are Hard to Secure

- Highly dynamic environment and unpredictable usage patterns by users
- End-Point Infections in enterprises
  - Up to 9% of the end-points in enterprises are found infected
- Best of breed antivirus, perimeter protection, and IDS/IPS do not provide 100% detection

Source: Damballa on Darkreading http://bit.ly/EntBot

#Hosts x #Vulnerabilities

=

Opportunity

What does a typical End-Point look like?

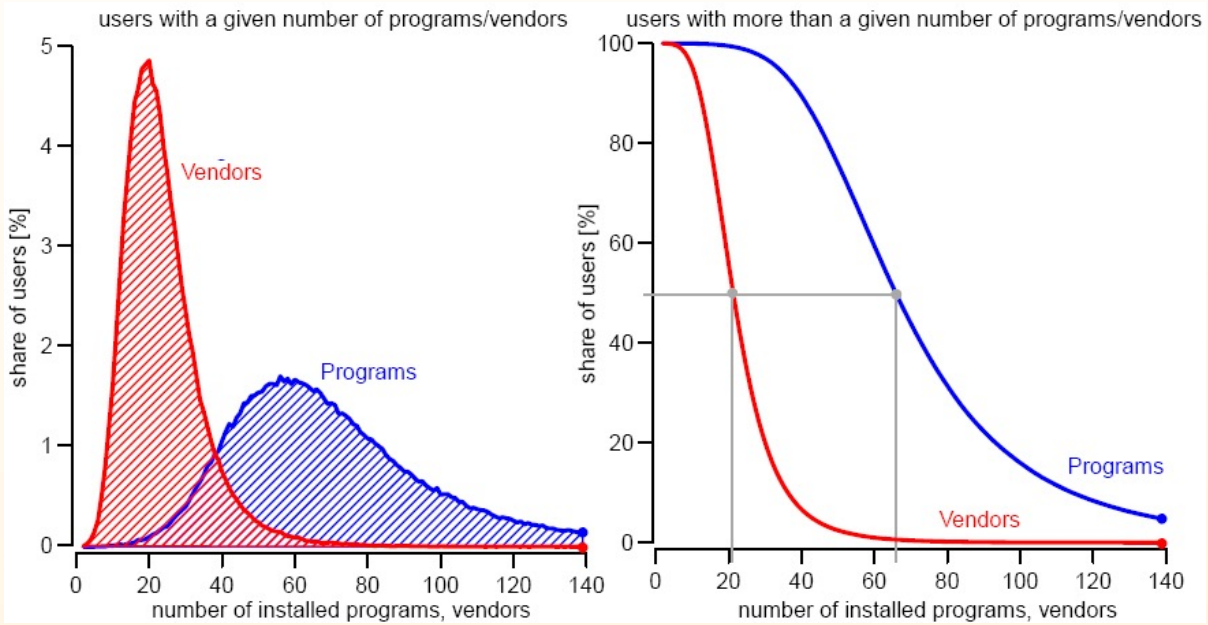
- Numerous programs and plug-ins installed
- How many programs do you think you have installed on your typical Windows machine?
- How many different update mechanisms do you need to keep this PC up-to-date?

Under the Hood of typical End-Points

- Secunia PSI is a lightweight software inspector (scanner) to
  - identify insecure programs and plug-ins
  - automatically install missing patches
- Based on our robust Corporate Software Inspector (CSI) technology
- The Secunia PSI is free for personal use
  with over 3 Million registered users in 2010
  http://secunia.com/psi

Software Portfolios …

- 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

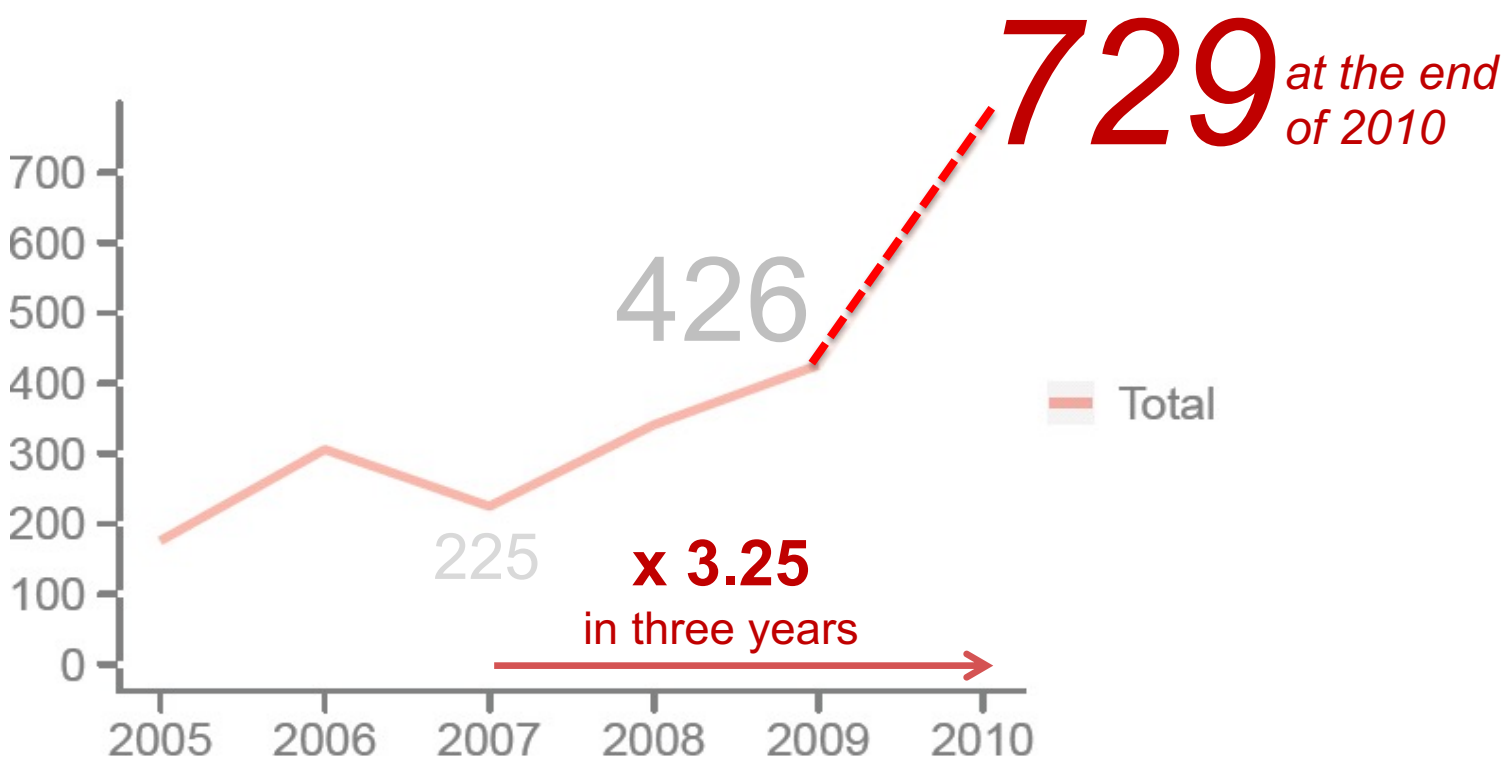
Analysis based on Secunia PSI scans in 2010

Typical End-Point Software Portfolio

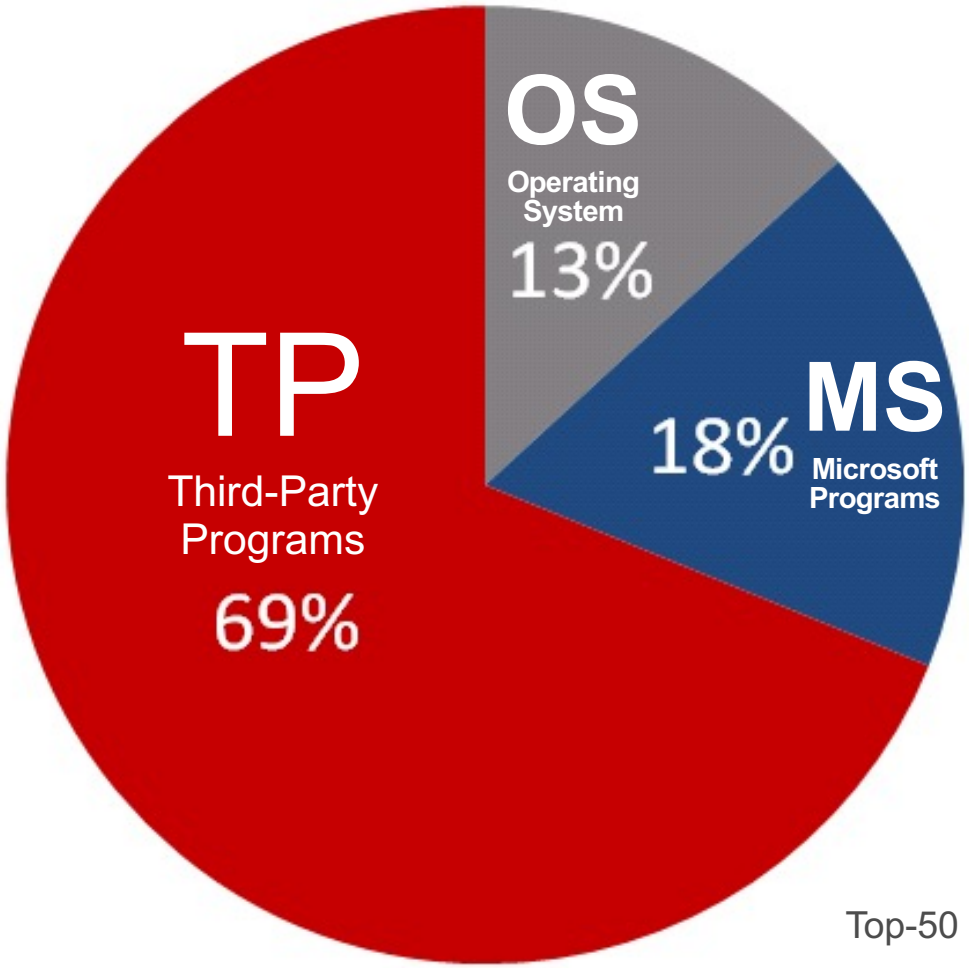
- The Top-50 Software Portfolio covers the 50 most prevalent programs to represent a typical end-point
  - It contains 26 Microsoft and 24 Third-Party (non-Microsoft) programs from 14 different vendors

An Alarming Trend …

- Vulnerabilities affecting a typical end-point increased 71% to 729 per year from 2009 to 2010



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

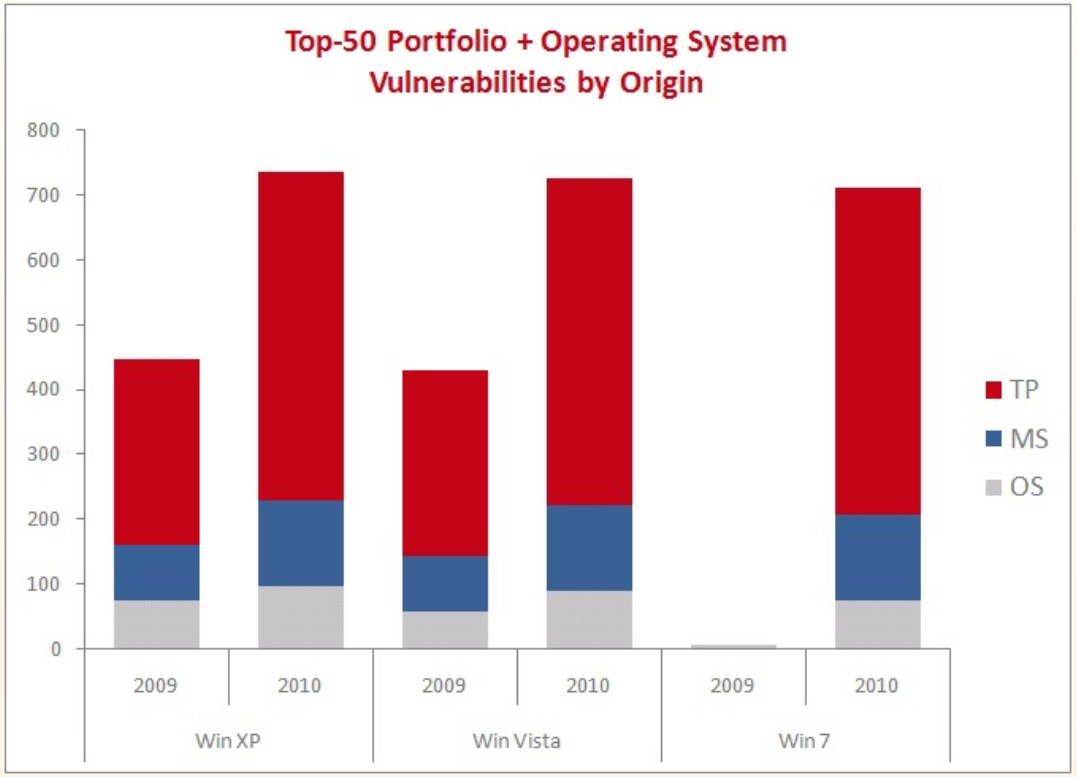


Top-50 Portfolio & Windows XP Vulnerabilities in 2010

Third-Party Programs Rule ..

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

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



Updating a typical End-Point …

To keep a PC with the Top-50 portfolio fully patched, the user has to manage a total of

14 different update mechanisms

1

Update Mechanism

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

13

Update Mechanisms

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

Cybercriminals know

patch available

≠

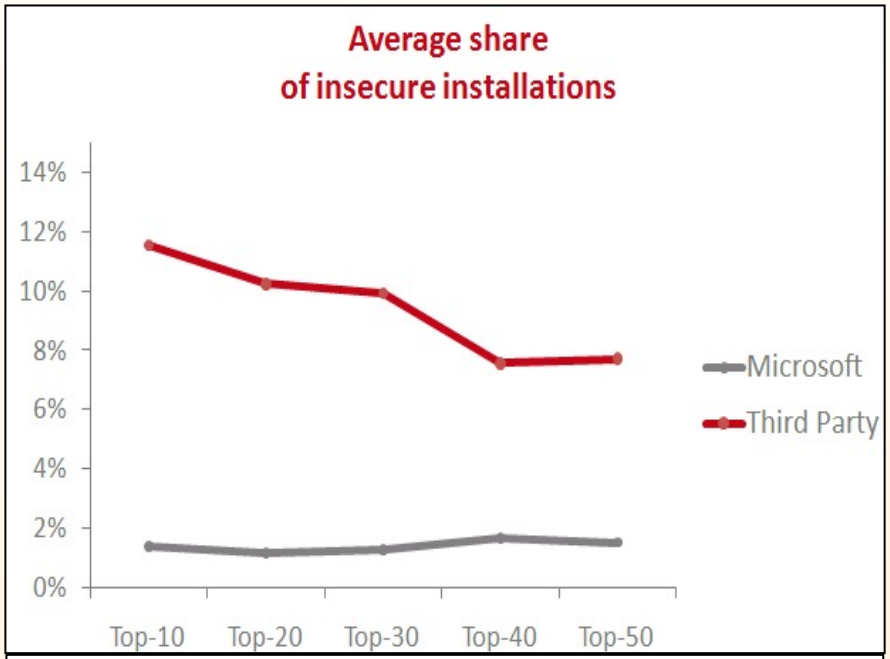
patch installed

Patch Complexity Hurts …

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

- Less than 2% insecure Microsoft programs

- 6%-12% insecure third-party programs



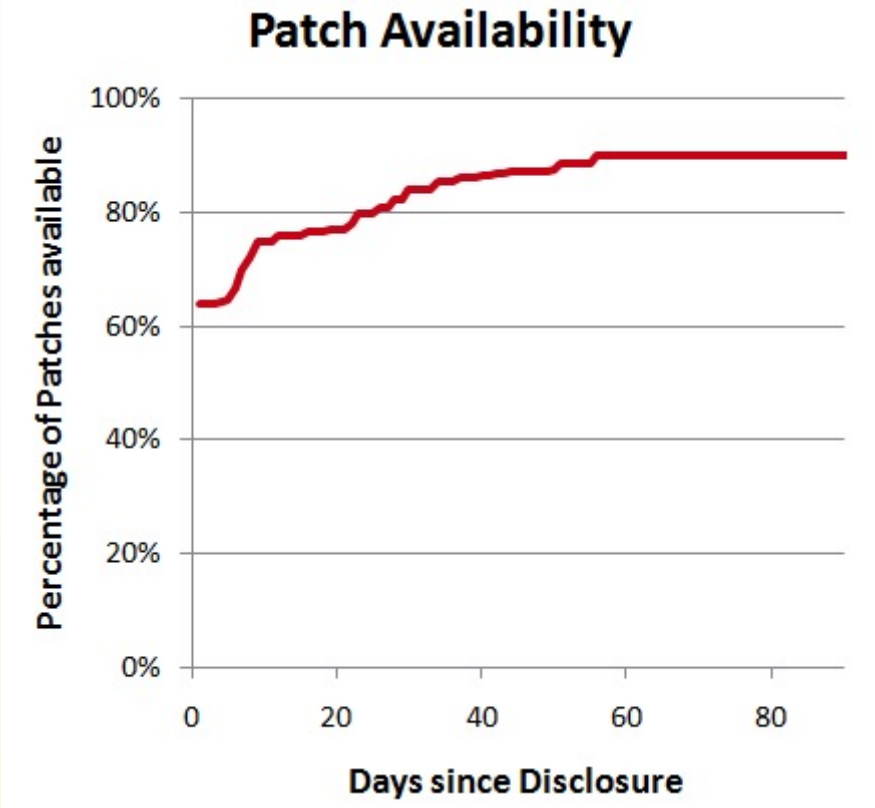
Average share of insecure programs in the Top-N Microsoft and Top-N Third-Party Programs

Source: Secunia PSI scans 2010/Q4

However, Patches are Available!

- Patch availability within N days upon vulnerability disclosure:

- 65% patch availability at disclosure
- 75% patch availability within 10 days
- 90% patch availability within 56 days



Top-50 Portfolio & Windows XP

#Hosts x #Vulnerabilities
x {Complexity to stay secure}
=
Opportunity

Cybercriminals' Attack Tactics

- Multiple variants of a particular malware agent are automatically created in advance of the attack:
  - only variants that pass quality assurance (= bypass antivirus) are used for attacks
  - each new variant is released at scheduled intervals to constantly remain ahead of antivirus protection updates

Malware is prevalent and can be produced to successfully bypass traditional perimeter defenses.

A patch provides
better protection
than thousands of signatures

it eliminates the
root cause

Conclusion

- 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 backdoor remains widely open
- Patching should be prioritized as a primary measure given its effectiveness to neutralize attacks
- Controlled identification and timely patching of all programs, incl. 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