

Real Performance?

Ján Vrabc vrabc@eset.sk

David Harley धारley@eset.com



Agenda

Introduction

Detection vs. Whole Product Test

Performance Tests

Black box testing suites

Irrelevant Testing

Types of users

Introduction

- Detection vs. performance testing
- Evaluation – Testing
- Buying decisions
- Missing guidelines
- Own testing procedures
- AMTSO

Detection performance isn't enough in itself

- Usability, ergonomics and configurability
- Functional adaptation
- Responsiveness to the needs of and changes in the organizational environment or infrastructure
- Responsiveness or adaptability to business needs

Detection Testing Versus Whole Product Testing

- More functions
- Impact on performance
- Interactions
- “Out of the box” settings
- Different view

Detection Testing Versus Whole Product Testing

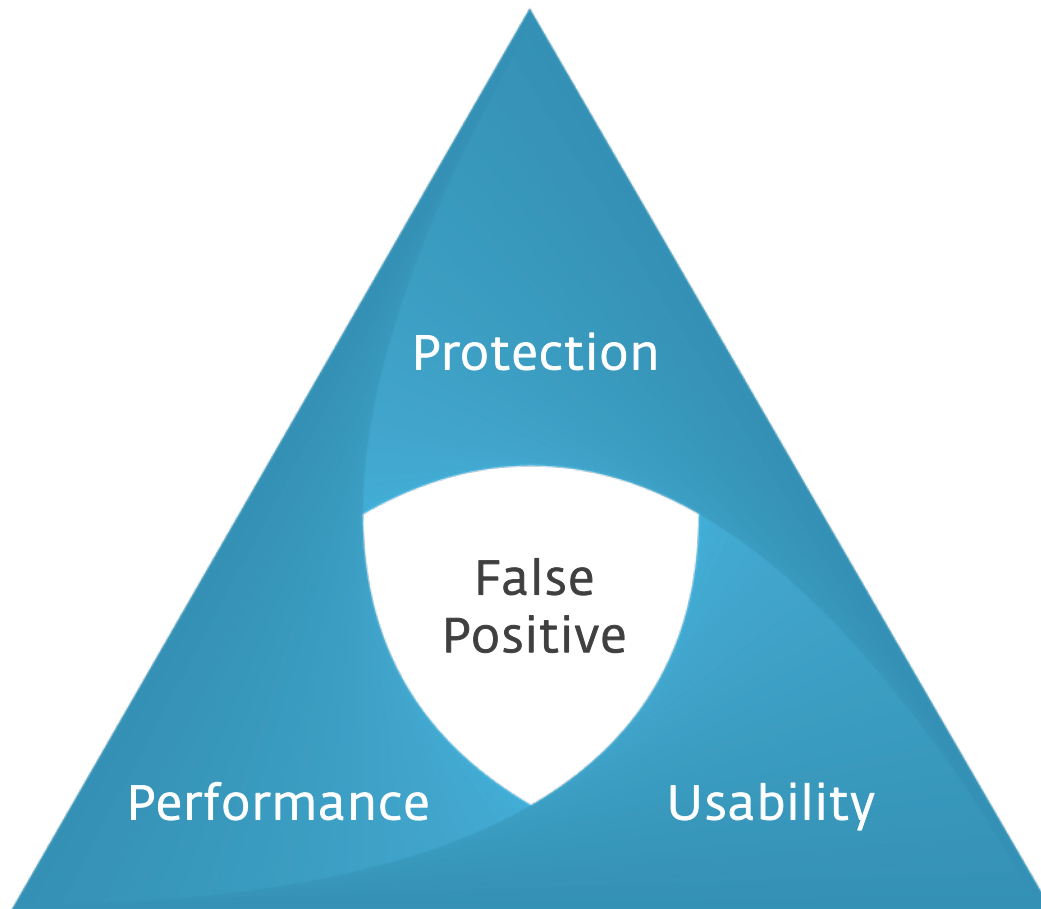
TESTER FOCUS



USER VIEW



Balanced Product



Scanning Throughput

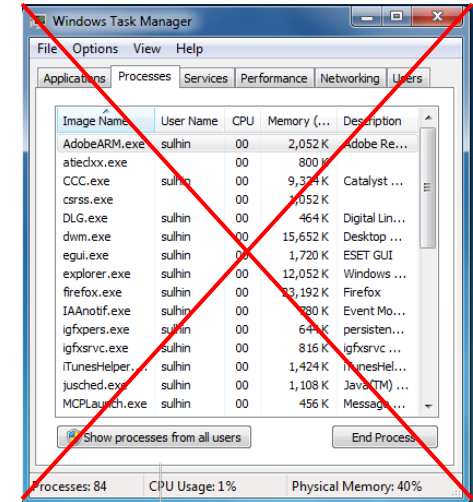
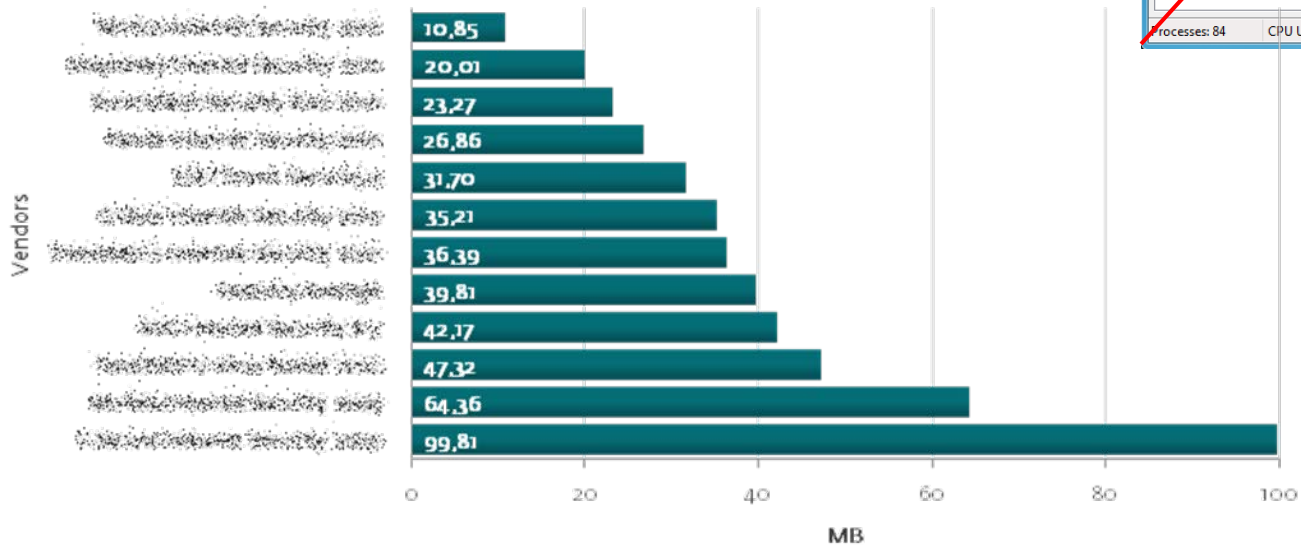
- Static scanning
- Samples - Clean Set
- Representative set
- Skip over files
- Multiple measurements
- First and following scans
- Hashing – Faster – Secure?



Memory Usage

- System is in idle state
- Windows Task Manager
- Hidden processes, 10 MB antivirus 😊

Memory Usage while Idle



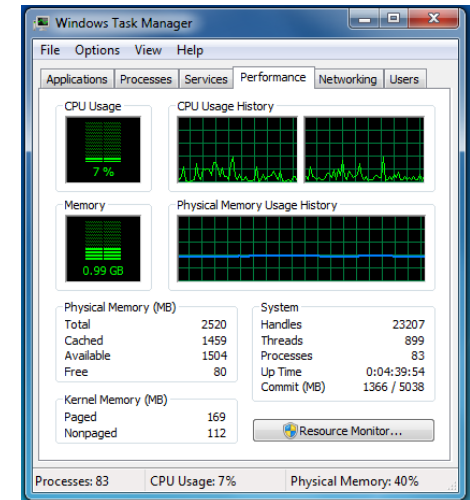
Memory Usage

- System in idle
- Several readings
- Reserved memory

CC of system with installed solution

-CC of clean system

Memory Consumption



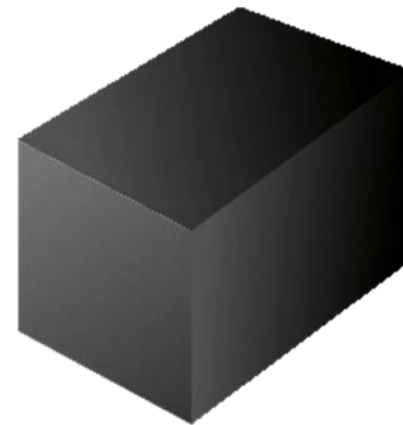
System Boot Speed

- Active on a system at an early stage
- When to stop the measurement?
- Antivirus presence detector
- Idle state of system



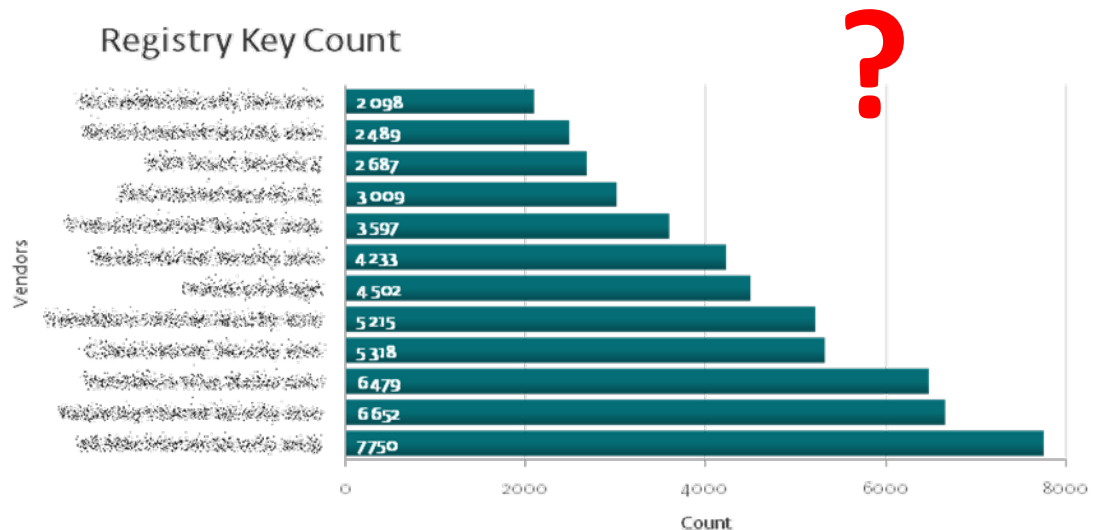
Black Box Testing Suites

- Instant Testing Tools
- World Bench or Passmark
- Focused on hardware
- White listed
- Error bigger then difference
- Interpretation of results



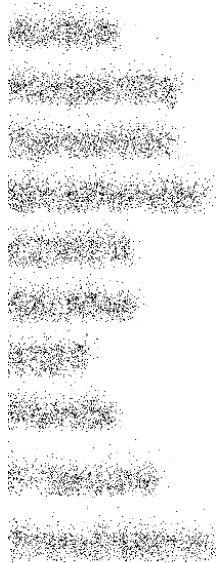
Irrelevant Testing

- False tests
 - Registry Key Count
 - Process Count
- No effect on computer performance
- Improved product rating



Magazines Results

- German computer magazine reviews
- Varied results
- Confused reader



	Computer Bild	Chip	PC Magazin	PCWELT	Protectstar	PCtipp	PCNEWS COM!
	7	1	7	1	3	3	4
1	6	5	4	6	2	1	7
2	1	1	2	4	2	4	1
3	3	1	3	5	3	4	6
4	4	4	1	2	1	1	3
5	8	12	10	8	3	5	x
			8	3	4	1	9
	2	6	6		4		5
		7	5	7	3	2	2
		7	9		3		8

Malware Performance Testing by User Type

Consumer



- Surfer
- Gamer
- Worker

Corporate



- Users
- Administrators

Consumer



All

- Boot time
- Memory consumption
- Installing common software applications
- Copying files to the system or to and from a local network resource

Surfer

- Browsing of web pages from proxy server
- Browser start-up time
- Viewing video files streamed from a Web server

Consumer



Gamer

- Latency on the network
- Degradation of frame per seconds

Worker

- Downloading emails from server
- Email clients start-up Time of opening, closing, saving and copying documents
- Editing video and audio files
- Converting from one format to another
- Start-up times of specific applications

Corporate

Users

- Simulation of work with common business software
- Time taken to open, process and close single or multiple documents and applications
- Network performance
- Accessing email or messaging services
- Web browsing
- Designing internal applications, procedures and implementations in-house.



Administrators

- Performance on File and mail servers, gateways

Conclusion

- Testing with pitfalls
- Valid and objective techniques
- Guidelines
- More focus on Whole Product Testing

The logo for the Anti-Malware Testing Standards Organization (amtso) consists of a horizontal bar with a red-to-white gradient on the left and a solid dark blue section on the right. The text 'amtso' is written in white lowercase letters on the red gradient part.

amtso

Anti-Malware Testing Standards Organization

The Nine Principles 1/2

1. Testing must not endanger the public.
2. Testing must be unbiased.
3. Testing should be reasonably open and transparent.
4. The effectiveness and performance of anti-malware products must be measured in a balanced way.
5. Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.

The Nine Principles 2/2

6. Testing methodology must be consistent with the testing purpose.
7. The conclusions of a test must be based on the test results.
8. Test results should be statistically valid.
9. Vendors, testers and publishers must have an active contact point for testing related correspondence.

AMTSO Compliance

- Technically, there's no such thing (yet)
- The Review Analysis Board *can* assess whether a test report is compliant with the nine principles:
<http://amtso.org/amtso---download---amtso-analysis-of-reviews-process.html>
- Two analyses (near-)completed to date:
 - NSS Labs
 - Dennis Publishing

AMTSO Documentation

<http://amtso.org/documents.html>

Documents and Principles

These documents are either fully published or work in progress specifying AMTSO Principles and Guidelines related to testing.

[Virus Bulletin Spotlight article on AMTSO](#)

What AMTSO has achieved so far, and what might lie ahead. David Harley, AMTSO lutely Fabulous, January 2010, Virus Bulletin. Copyright is held by Virus Bulletin Ltd, but is made available on this site for personal use free of charge by permission of [Virus Bulletin](#).

[AMTSO Fundamental Principles of Testing](#)

AMTSO Fundamental Principles of Testing as approved by the AMTSO meeting held in Oxford 31st October 2008.

[AMTSO Best Practices for Dynamic Testing](#)

AMTSO Best Practices for Dynamic Testing as approved by the AMTSO meeting held in Oxford 31st October 2008

[AMTSO Best Practices for Validation of Samples](#)

AMTSO Best Practices for validation of samples as approved by the AMTSO meeting held in Budapest 7th May 2009

AMTSO Documentation

<http://amtso.org/documents.html>

[AMTSO Best Practices for Testing In-the-Cloud Security Products](#)

AMTSO Best Practices for Testing In-the-Cloud Security Products as approved by the AMTSO meeting held in Budapest 7th May 2009

[AMTSO Analysis of Reviews Process](#)

AMTSO Analysis of Reviews Process as approved by the AMTSO meeting held in Budapest 7th May 2009

[AMTSO Guidelines for testing Network Based Security Products](#)

AMTSO Guidelines for testing Network Based Security Products as approved by the AMTSO meeting held in Prague 13th October 2009

[AMTSO Issues involved in the "creation" of samples for testing](#)

AMTSO Issues involved in the "creation" of samples for testing as approved by the AMTSO meeting held in Prague 13th October 2009

Thank you for your attention

Questions?

Ján Vrabec vrabec@eset.sk
David Harley धारley@eset.com



References

- AMTSO (2010a). AMTSO Whole Product Testing Guidelines (in preparation)
- AMTSO (2010b). AMTSO Performance Testing Guidelines (in preparation)
- ESET Research (2010). Retrieved 10th March 2010 from <http://www.eset.com/blog/2010/01/25/generalist-anti-malware-product-testing>
- AV Comparatives (2009) Retrieved 10th March 2010 from http://av-comparatives.org/images/stories/test/performance/performance_deco9.pdf
- Harley, D. (2009a). Making Sense of Anti-Malware Comparative Testing. Information Security Technical Report. Retrieved 10th March, 2010 from <http://dx.doi.org/10.1016/j.istr.2009.03.002>, Elsevier.
- Harley, D. (2009b). Execution Context in Anti-Malware Testing. Conference Proceedings for 18th EICAR Annual Conference. Retrieved 10th March 2010 from <http://smallbluegreenblog.wordpress.com/2009/05/15/execution-context-in-anti-malware-testing/>
- Lee, A.J. & Harley, D. (2007). Antimalware Evaluation and Testing. In D. Harley (Ed.) AVIEN Malware Defense Guide for the Enterprise (pp. 441-498): Syngress
- Vrabec, J. (2010). Generalist Anti-Malware Testing (In preparation)