NORMAN®
Celebrating 25 years

AMTSO

The status right now

Righard J. Zwienenberg
Chief Research Officer
Righard J. Zwienenberg
Chief Research Officer

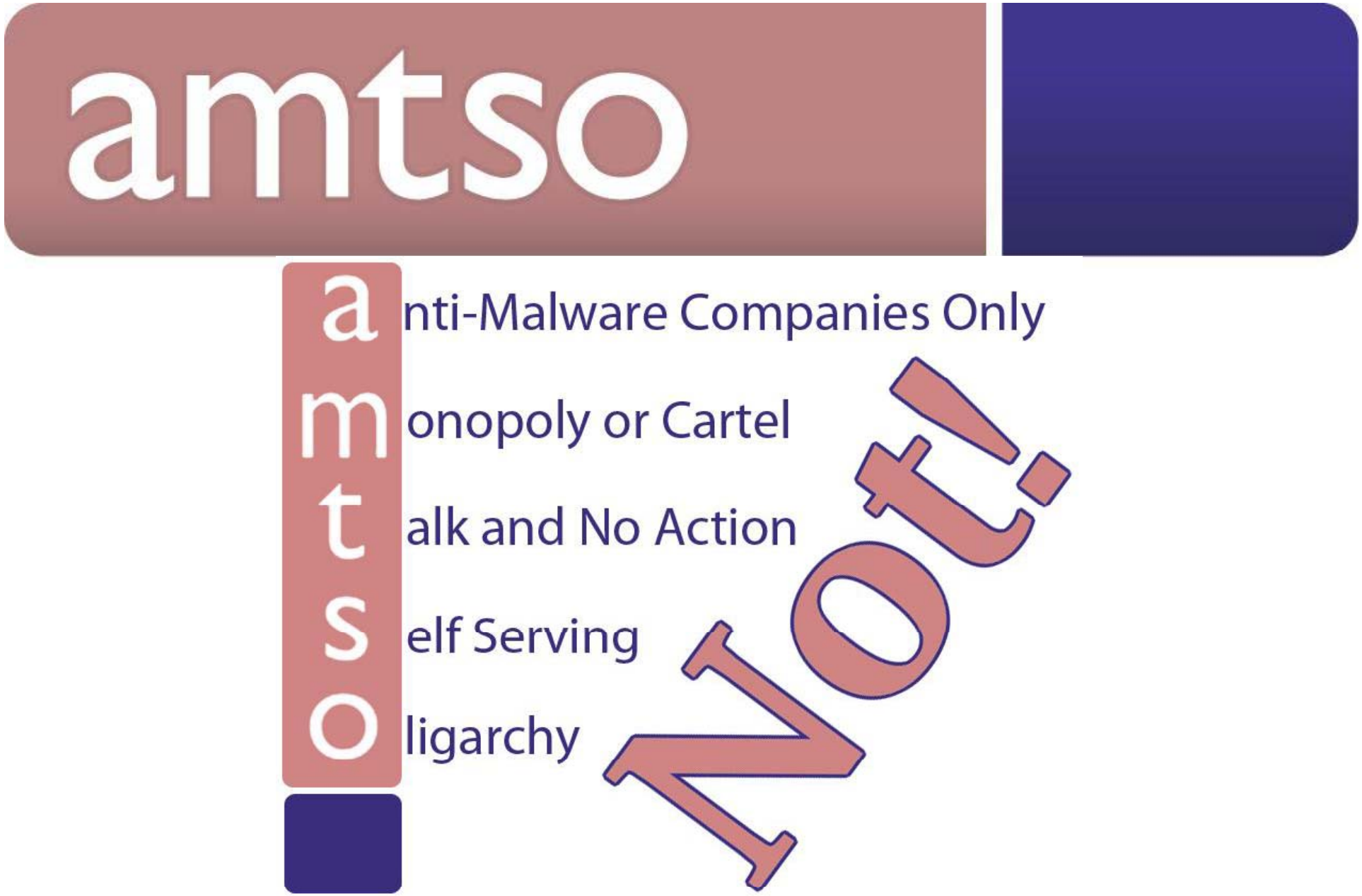
Anti-Malware Testing Standards Organization

amtso

Agenda

- In short: What is AMTSO?
- The history: The What, Why and How on AMTSO
- The now: documents finished
- The now: Work in Progress
- The future
- Membership

Anti-Malware Testing Standards Organization


amtso
anti-Malware Companies Only
monopoly or Cartel
talk and No Action
self Serving
oligarchy
Not!
Anti-Malware Testing Standards Organization

amtso

The history

- 2007: Reijkavik: First International CARO Workshop
- 2007: Seoul, AVAR Conference
- 2008: Bilbao, the “conception” of AMTSO

Anti-Malware Testing Standards Organization

amtso

The history

- 2008: May, AMTSO incorporated in California, USA as a non-profit organization and official elections were held where the interim board was replaced with an official chosen board. AMTSO was officially born and started to work on the Standard Documents.

Anti-Malware Testing Standards Organization

amtso

The history

- Board of directors, 9 members
  - 1.Righard J. Zwienenberg
  - 2.David Harley
  - 3.Stuart Taylor
  - 4.Roel Schouwenberg
  - 5.Mark Kennedy
  - 6.Gabor Szappanos
  - 7.Karel Obluk
  - 8.Andreas Marx
  - 9.Igor Muttik

Anti-Malware Testing Standards Organization

amtso

The history

- Advisory board, 7 members
  - 1.Neil J. Rubenking, PC Mag Digital Network
  - 2.Ivan Krstic, former Chief Security Architect, One Laptop Per Child
  - 3.Dr. Jose M. Fernandez, Ecole Polytechnique de Montreal
  - 4.Thorsten Holz, University of Mannheim
  - 5.Dr. Herbert H. Thompson, PeopleSecurity
  - 6.Maxim Weinstein, Stop Badware.org., Berkman Center for Internet and Society at Harvard University
  - 7.Jaimee King, independent

Anti-Malware Testing Standards Organization

amtso

AMTSO aims to....

- Improve testing methodology across the board:
  - Objectivity
  - Quality
  - Relevance

Anti-Malware Testing Standards Organization

amtso

Target Membership

- Testing Organizations
- Security Vendors
- Academia
- Reviewers and Publications
- …

Anti-Malware Testing Standards Organization

amtso

The members

AhnLab, Alwil Software, ARCABIT, AV-Comparatives, AVG Technologies, AVIRA, AV-TEST.org, Bit9, BitDefender, CA, Inc., Cascadia Labs, Comodo Security, Inc., Dennis Technology Lab, ESET, F-Secure, Hispasec, IBM, ICSA Labs, Ikarus Security Software, Kaspersky Lab, KingSoft, K7 Computing Private Ltd, Lavasoft AB, Mario Vuksan, McAfee, Norman, NSS Labs, Panda Security, PC Security Labs, Sophos Plc, Symantec Corporation, TrendMicro, Vesselin Bontchev, Veszprog Ltd., Virus Bulletin, VirusBuster, Webroot Software Inc., West Coast Labs

Anti-Malware Testing Standards Organization

AMTSO Charter

- Provide a forum for discussions related to the testing of anti-malware and related products
- Develop and publish objective standards and best practices for testing of anti-malware and related products
- Promote education and awareness of issues related to the testing of anti-malware and related products, and provide tools and resources to aid standards-based testing methodologies
- Providing tools and resources to aid standards-based testing methodologies
- Providing analysis and review of current and future testing of anti-malware and related products

Anti-Malware Testing Standards Organization

amtso

Documentation Deliverables

- Available (http://www.amtso.org/documents.html)
  - AMTSO Fundamental Principles of Testing (Oct 2008)
  - AMTSO Best Practice in Dynamic Testing (Oct 2008)
  - AMTSO Best Practices for Validation of Samples (May 2009)
  - AMTSO Best Practices for Testing In-the-Cloud Security Products (May 2009)
  - AMTSO Analysis of Reviews Process (May 2009)

amtso

The Nine Principles

- **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.**
- **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.**

Anti-Malware Testing Standards Organization

amtso

Principle 1:Testing must not endanger the public

- Follow safe procedures to ensure that test samples don't endanger the community at large.
- This section also talks about the highly contentious topic of *creating* malware to test with.

amtso

Principle 2: Testing must be unbiased

- Each product must be treated equally.
- The tester is obliged to conduct the test ethically, and present truthful and unbiased results.

amtso

Principle 3: Testing should be reasonably open and transparent

- Information needed might include:
  - product version and update status
  - configuration
  - test conditions
  - source and selection of samples and how they were validated
  - methodology
  - calculation and interpretation of results.

amtso

Principle 4: The effectiveness and performance of anti-malware products must be measured in a balanced way

- May be misleading to summarize product efficacy with a single measurement

amtso

Principle 5: Validation and Classification

- “Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.”

amtso

Principle 6: Testing methodology must be consistent with the testing purpose

- Tests must address the intended or stated purpose of the publisher's related review or article...publishers should state the objective of their tests clearly…test methodology should be consistent with the stated test objective.

http://www.smallblue-greenworld.co.uk/AV_comparative_guide.pdf

amtso

Principle 7: The conclusions of a test must be based on the test results

- This principle addresses a common high level problem with publishing conclusions alongside testing data that are not supported by those data. (For example, drawing broad and/or inaccurate conclusions from narrow test data.)

amtso

Principle 8: Test results should be statistically valid

- For instance, based on a sufficient quantity of validated test samples.

http://www.mcafee.com/common/media/vil/pdf/imuttik_VB_conf_2001.pdf

amtso

Principle 9: Active Contact Point

- "Vendors, testers and publishers must have an active contact point for testing-related correspondence"
- Basically, if you're going to publish test results, you should be prepared to answer comments and queries.

amtso

Next Steps

1. Make testers out of the mainstream more aware of their responsibilities to their audience.
2. Make it easier for audiences to distinguish between good and not-so-good tests and reviews
3. Build on co-operative relationships between the vendors

Anti-Malware Testing Standards Organization

amtso

Analysis of Reviews Process

- The Subject Review must be primarily focused on an anti-malware product or service or, in the case of Subject Reviews of solutions which encompass multiple products or technologies, the Subject Review must give significant consideration to anti-malware functionality.

amtso

Analysis of Reviews Process

- The Subject Review must either be due for imminent publication or else must be already publicly available, either free of charge or by subscription.

amtso

Analysis of Reviews Process

- The AMTSO Guidelines and Principles must be of relevance and applicable to the Subject Review for which analysis is requested.

amtso

Analysis of Reviews Process

- Target: the fundamental purpose of such a requested analysis will be to publish an Analysis which compares the Subject Review to AMTSO Guidelines and Principles as currently in effect. The Board shall impartially review and accept or decline each Analysis Request

amtso

Analysis of Reviews Process

- There shall be no fee associated with the Analysis Request, *Analysis or process associated therewith.*

amtso

Analysis of Reviews Process

- The AMTSO Analysis makes no judgments or endorsements of the Reviewer or Product(s) under review. The Analysis only makes representations as to compliance or noncompliance to specific AMTSO Principles and Guidelines. AMTSO members, Reviewers, Analysis Filers, organizations, or individuals must not misrepresent these findings with statements such as “AMTSO says XYZ product is the best”, “ABC Testlab is AMTSO-approved”.

amtso

Work in Progress

- Glossary/Definitions
- Static Testing
- On-demand testing versus whole product testing
- Issues around creating malware for testing
- How to obtain and validate malware samples

Anti-Malware Testing Standards Organization

amtso

Membership

- Website: http://www.amtso.org/membership.html

- Next meeting: 12 and 13 October in Prague http://www.amtso.org/meetings.html

Anti-Malware Testing Standards Organization

Questions?

http://www.amtso.org

Anti-Malware Testing Standards Organization