The Daze of Whine and Neuroses

(But Testing Is FINE)

David Harley CITP FBCS CISSP
ESET Senior Research Fellow

Larry Bridwell
Global Security Strategist, AVG Technologies
Agenda

• Introduction
• A little history of testing
• AMTSO
  – Tester/Vendor continued cooperation?
  – Useful Still?
• Future of Comparative Testing
Testing is FINE

F = Freaked Out  F**ked Up
I = Insecure
N = Neurotic
E = Emotional
Testing Types

• Comparative reviews
• Certification/Validation
• Academic
• In company/corporate
...is the testing really FINE

- Caro workshop May 2007
- In Iceland and sponsored by F-Prot
- 2 days of presentations on Testing
- 2 days of discussing testing in smaller groups
- Panda sponsored conference Jan 2008
- Anti-Malware Testing Standards Organization
Conflicts of Interest

- Testers versus vendors
- Samples and maURLS: share and share alike?
  - Testers and vendors use some of the same resources
  - Some testers solicit samples/URLs from vendors
  - Some testers verify samples with vendors
Rule of Nines

• 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.
Interesting Questions

• Who’s better at collecting and classifying samples?
• Who knows the technology better?
• How can both parties share without compromising independence?
• Should they even try?
Interesting Questions [2]

• How can both parties share without compromising independence?
• Should they even try?

$$$$$$
What else do they have in common?
Conflicts of Interest

- Testers versus publishers
- Testers versus vendors
Piggy in the Middle
Conflicts of interest

• Critics versus vendors
• Everybody versus the vendors!
• Members versus subscribers
Members versus Subscribers

• Members face a heavy burden of expectation
• Subscribers pay less, participate less, and we expect less. But...
AMTSO is...

- More than the sum of its members
- More than the sum of its Board of Directors
- Individual members of either don’t automatically speak for AMTSO
AMTSO Compliance

• No testing is generically “AMTSO compliant” by virtue of its being conducted by a member of or subscriber to AMTSO: there is at present no such status defined. The term "AMTSO compliant" has no formally defined or approved meaning, and its use is deprecated pending a definition established by AMTSO itself.
Vendor Black Ops

• Members and subscribers may not use the term AMTSO-compliant or otherwise to negotiate with, persuade or coerce testers into changing test results that they feel has disfavoured particular products or services.
I AMTSO well-connected

- Goodwill Hunting
- Demonstrating Good Faith
We all need to keep our balance here
Conclusion

**F** = Formational or Formulation

**I** = In Process

**N** = Nascent

**E** = Emotional
Questions

Larry Bridwell
larry.bridwell@avg.com

David Harley
david.harley@eset.com

WHEW!!