

## SPOTLIGHT

### AMTSOLUTELY FABULOUS

David Harley  
ESET, USA

*The Anti-Malware Testing Standards Organization (AMTSO) was formed following a 2007 CARO workshop aimed at discussing ‘best practice’ and common flaws in anti-virus testing methods. A selection of participants from the workshop decided to join forces and in January 2009 more than 40 security software experts and anti-malware testers from around the world met to formalize the charter of the Organization. Since its inception, the AMTSO has outlined its charter, held regular meetings, produced a range of standards documents and continues to work towards raising the overall standard of testing. However, there is still confusion as to what the organization does and stands for. David Harley provides his take on what AMTSO has achieved so far, and what might lie ahead.*



Does Figure 1 represent your perception of the Anti-Malware Testing Standards Organization (AMTSO) [1]? Many people with an interest in anti-malware testing are now watching the organization with keen interest, but somewhat in a state of confusion.



Figure 1: AMTSO: the view from the T-shirt.

### WHINE AND DINE

Some see AMTSO as a group of anti-virus vendors meeting to whine about how awful testing is; others have a clearer view of who is participating, but think of it as a testing organization in its own right – or expect it to transform into a full-blown standards development organization like ISO, or a full-time compliance monitoring agency. I don't

presume to speak for AMTSO, but let me give you my own views on what has been achieved so far and what might lie ahead.

AMTSO represents a productive (and open – more members are always welcome) alliance between the anti-malware industry, mainstream testers and publishers, all of whom have had to invest much time and effort into adjusting to new threat trends. Vendors have done so by working on enhanced approaches to detection; testers, reviewers and publishers have done so by developing realistic criteria and methodologies for evaluating and comparing re-engineered technologies. The organization also benefits from the input of an advisory board [2] consisting of people who, despite their knowledge and experience of the anti-malware industry, have no vested interest in promoting it. AMTSO has always felt that the presence of this group is essential to the purpose and functioning of the organization, defending the interests of the community at large against AMTSO's becoming a clique of self-interested vendors.

### ENLIGHTENED SELF INTEREST

Of course, it is inevitable that vendors will be (self-)‘interested’, but most believe that they have as much to gain from a higher standard of testing across the board as anyone else [3]. In any case, an organization without the accumulated experience of the anti-malware research community would be hard-pressed to maintain credibility, as it would lack input from the people who know the most about the technology under test.

Central to AMTSO's purpose is the recognition among the security community (including mainstream professional testers) that traditional static testing (a.k.a. throwing every available malicious program at an on-demand scanner to see how many it detects) is no longer a fully effective measure of a product's capabilities – if it ever was.

### GLUT... GIVE ME GLUT AND NOTHING BUT...

In a threat landscape where tens of thousands of new samples [4] – most of which are non-viral (that is, trojans of some sort rather than self-replicating malware) – are seen on a daily basis, the leisurely testing methodologies of yesteryear are of limited use. However, more dynamic testing methods that reflect the complexities of a constantly shifting threatscape (and increasingly, cloud-based technologies) are themselves complex and resource-intensive. Even testers who are aware of the need to move towards dynamic testing are often deterred by the resource implications and the technical difficulties.

## INFORMATIONAL LOAD BALANCING

Clearly, there is a need for information sharing and discussion if the testing industry is to progress. AMTISO offers a forum for expert discussion as the testing industry moves towards more relevant testing methods, with input from the anti-malware sector of the security industry as well as from some of the most experienced mainstream testers.

Perhaps AMTISO's core function is to raise the overall standard of testing, through discussion (and there's been plenty of that!), by developing standards and documenting good practice, by encouraging the provision of tools and other resources, by providing analysis and review of tests, and, perhaps most significantly, through education. One way to raise awareness is by providing sound information from authoritative sources. To this end, AMTISO members have put together a repository of documents [5]. A particularly significant item is a testing principles document [6] that provides a high-level view of the basic rules of sound anti-malware testing. These are not tablets of stone, but documents that may be amended over time to adapt to changing circumstances and technologies.

## TESTING, TESTING, 1, 2, 3

Software testing has never been a particularly easy discipline, and security product testing poses particular challenges, since the technical aspects of attacks and countermeasures are not always well understood (or, indeed, communicated by the industry). For a long time, it seemed as though the anti-virus industry was eager to complain about bad tests, but unresponsive when asked 'so how would you *like* us to do it?' [7].

AMTISO has made moves to overturn this perception by providing copious documentation on basic principles and on specific testing issues. These don't provide the wannabe tester with everything he could ever need in order to become a credible tester, but they do at least provide a basis for communication between AMTISO and testers (and other interested parties) currently outside the organization. It is no longer possible for anyone to claim that there is no useful, impartial information on testing to be found outside the charmed circle of vendors and mainstream testers. Even testers outside the relatively close-knit security community can draw on this resource to enhance the value of their testing, and in turn, their audiences can gain better understanding of how testing works.

## NEGATIVE POLARITY

Inevitably, some people have anticipated a more negative and authoritarian approach from AMTISO, and in some

cases there has been disappointment that it has not been more ready to wield the stick than the carrot. There seems to be a common perception that



AMTISO either has or *should have* set itself up as the AV industry's police force, to monitor and enforce good testing methodologies – after all, the name of the organization includes the word 'standards' (not 'guidelines', 'suggestions', or even 'good practice'). However, AMTISO is *not* the AV industry, and though that industry's interests are certainly represented, they are secondary to the interests of the community at large. While there's a place for both the carrot and the stick, AMTISO's best course right now is to establish dialogue and consensus across the community, rather than to be the ultimate authority on good and evil in testing.

## CONCLUSION

Anti-malware testing is not as easy as most people think it is (in fact *all* product testing is harder than most people think): it takes skill, knowledge, care and significant resources to perform a test that offers good guidance on a product's capabilities rather than subjective opinion based on misinterpretation and unrealistic assumptions. All too often, a single data set is used by different groups to support very different conclusions.

Perhaps the best services AMTISO offers to the community in the short term can be summarized as follows:

- Testers are not (only or primarily) accountable to the security industry, but to their audiences, who expect (sometimes naively) to be guided by objective, informed evaluation, not to be misled by personal prejudice. Of course, it's not only testers who need to know this, but also the public, who are often prepared to believe anything anyone says about a product as long as that person claims to have no connection with the industry [8].
- AMTISO has already made a difference simply by providing a platform for debate and a public resource of which testers can make good use, but it also has the potential to provide a better yardstick for the evaluation of tests. While it's not yet clear exactly what AMTISO compliance is, let alone how to measure it, many groups seem to want it, either so that they can use it as a metric, or so that they can demonstrate compliance.
- AMTISO does not certify tests or testers, and is not really in a position to adopt a compliance enforcement

role until there are formal standards against which to apply certification. However, AMTSO's good practice guidelines describe the principles that a sound tester would normally be expected to follow. These principles form a viable basis for a number of approaches to improving accountability: AMTSO's Review Analysis Board [9] is starting to use them as a measure of the accuracy of a test or review, while a self-assessment process has also been proposed. This would enable a testing group to demonstrate its intent to comply with AMTSO guidelines and willingness to undergo some form of verification. In the longer term, there are certainly arguments for a formal certification process: hopefully AMTSO would participate or perhaps even initiate such a process.

By stressing the constructive aspects of AMTSO's mission to improve specific methodologies (notably, hybrid and dynamic testing) and community awareness of the problems and of the solutions, the organization hopes to encourage all interested parties to follow and participate in the debate. After all, it's to be expected that as AMTSO gains traction, it will be harder for testers and reviewers to claim credibility without demonstrating awareness of the organization's aims and making a verifiable effort to follow them. Now is the time for other players wishing to be heard in the debate to raise their hands and voices.

## REFERENCES

- [1] <http://www.amtso.org/>.
- [2] <http://www.amtso.org/amtso---boards---advisory-board.html>.
- [3] Harley, D.; Lee A. Who will test the testers? Proceedings of the 18th Virus Bulletin International Conference, 2008.
- [4] Harley, D.; Bureau, P-M. A Dose By Any Other Name. Proceedings of the 18th Virus Bulletin International Conference, 2008.
- [5] <http://www.amtso.org/documents.html>.
- [6] <http://www.amtso.org/en/amtso---download---amtso-fundamental-principles-of-testing.html>.
- [7] Harley, D. The Game of the Name: Malware Naming, Shape Shifters and Sympathetic Magic. 3<sup>rd</sup> Cybercrime Forensics Education & Training Conference, 2009.
- [8] Harley, D. I'm OK, You're Not OK. Virus Bulletin, November 2006, p.6.
- [9] <http://www.amtso.org/pr-090519.html>.