

# CONFERENCE REPORT 1

## CARO MIO, AMTSO MON AMOUR

David Harley  
ESET

A researcher's lot is not an easy one, with frequent treks to be made both virtually and in reality across time zones in an attempt to keep up with current threat and research trends. Sometimes, though, one comes across a conference or workshop where a happy combination of social networking, the exchange of solid information, great entertainment and a beautiful setting makes it all worthwhile. Last month I was fortunate enough to attend two such events held consecutively in Budapest: the annual CARO workshop, and the most recent AMTSO (Anti-Malware Testing Standards Organization) meeting.

### CARO

This year's CARO workshop was focused on the theme of exploits and vulnerabilities. The agenda displayed at <http://www.caro2009.com/> gives some idea of the range of sub-topics covered, and this report will cover a few of the highlights. As in previous years, it is likely that some of the presentations will be made available on the website, though the scope and nature of the workshop was such that some of the material may not be released publicly. While it is not appropriate for me to go into detail about technical issues that presenters may not wish to be made public, I hope it is acceptable for me to record some personal impressions of this lively event.



If anyone was going to have problems with a reluctant projector-to-laptop, it was probably as well that it was Righard Zwienenberg: in his keynote presentation he rose above the problems to give a typically entertaining, yet thought-provoking talk. His description of a call centre conversation about anti-skimming measures was a perfect illustration of a very common problem in security: the culture clash.

The keynote was followed by a consideration of recent vulnerabilities in *Adobe* products (especially *Acrobat/Reader* and *Flash*), an issue to which I've also been paying much attention in recent months. It may not be altogether fair to lay too much emphasis on the sheer number of such issues, but I was slightly shocked to see how many CVEs *Adobe* has notched up in 2008–2009. I would certainly hope in future to see a more coherent and proactive approach to security problems from *Adobe* than I think is currently the case.

Taking a very different angle, the next presentation considered the impact of zero-day vulnerabilities on

vendor stock market prices. To my surprise, I found this fascinating, and I will certainly be checking out some of the other research in this area that was cited by the presenter, Anthony Bettini.

The MS08-067 vulnerability is usually associated with Conficker, but it is useful to remember that the Conficker gang is not the only one skinning that particular cat, so Pierre-Marc Bureau followed the road less hyped as well as the established Conficker time line. However, as you might expect, the Conficker connection turned up on several occasions during the course of the workshop.

The afternoon's presentations, including Maksym Schipka's paper on *Office* exploits, maintained the high standards that had been set in the morning, but perhaps the show stopper was Peter Ször's 'Attacking the Cloud', a broadly based consideration of some potential weaknesses in cloud-based anti-malware technology. Controversially, some of the points he made referred to products that are already working in that space, provoking some lively discussion the following day.

For that evening we were all spirited away – that is, transported by bus – to an equestrian display, followed by an excellent dinner.

The next morning, Andreas Marx started off proceedings with a paper entitled 'Testing exploit-prevention mechanisms in anti-malware products'. The presentation drew comparisons with other pain points in the need for new approaches to anti-malware testing and set the tone for (or at least prefigured) the AMTSO meeting that was to follow the next day. Other presentations in the morning looked at PE and other vulnerable formats (AutoIt executables, NSIS installers and SWF files), plus a more specific look at Conficker in the context of vulnerability analysis. Abhijit Kulkarni and Prakash Jagdale followed up on work they had presented at AVAR last year on vulnerabilities in anti-malware scanners executing in 64-bit environments, and Ziv Mador presented a view of the current exploit landscape from *Microsoft*. In the final sessions, Roel Schouwenberg shared some juicy data and Nick FitzGerald talked about web exploit kits and their evolution, bringing to an end a typically exhausting but unmissable two-day brain-dumping session.

### AMTSO

The following morning it was back to the same room for a rather different event, though with a considerable



overlap in attendees. The AMTSO workshop was very much focused on organizational administration issues and

forthcoming deliverables, and it never ceases to amaze me that such an aggregation of strong-minded individuals are able to reach consensus on so many topics so (relatively) quickly. (I guess that not every horse designed by a committee is a camel.) Again, I should emphasise that these are very much personal impressions.

After a summary of the organization's recent activities, introducing such issues as the recently overhauled website at <http://www.amtso.org/> (it looks very good, but anyone with links to the documents hosted there might want to check that they still work), three more documents were discussed exhaustively and eventually accepted in principle by the membership:

- A document outlining the process for dealing with requests for review analyses. This establishes the mechanism by which interested parties can request an analysis of tests and reviews based on how closely they conform to AMTISO guidelines (see the 'Fundamental Principles of Testing' document at <http://www.amtso.org/documents.html>). I imagine that many will see this as a critical aspect of AMTISO's activities in the near future, and an essential step towards establishing compliance with AMTISO's principles as a 'must-have' for credible testing.
- A document outlining issues with and best practices for the testing of security products that use some form of 'in-the-cloud' distributed processing. Like dynamic testing, I expect this to be a growth area in comparative testing: it will be difficult and resource-intensive for testers to implement these approaches properly, but this document will offer solid guidance on evolving techniques that they will need to address sooner rather than later.
- A document suggesting methods by which samples can be validated. Again, I see this as a topic of crucial importance in testing: inadequate validation has undermined the viability of test after test over the years, and I regard it as one of the major issues that a testing standards body needs to address.

Work also continues on a glossary (yet another vital project, in my view) and on some other papers that are not yet ready for final approval, addressing topics such as sample generation (I can hear you groaning from here) and testing methods that take fully into account the holistic detection abilities of a product that so often get lost in a simple static test. Work has started on some new documentation.

Special thanks and congratulations to Gabor Szappanos and his colleagues for setting everything up for both events, and for looking after us all so well.