CONFERENCE REPORT 2

EICAR 2009 IN A NUTSHELL: ICH BIN EIN EICARER

Eddy Willems
Kaspersky Lab and EICAR, Belgium

The 18th EICAR conference took place last month in Berlin. Situated close to the fabulous Kurfürstendamm shopping street, as well as the famous Gedächtniskirche church, the Steigenberger hotel provided an ideal setting for the conference and the sun shone throughout the week.

The pre-conference programme, which ran for two days prior to the start of the conference, featured a number of workshops including an interesting tutorial about JavaScript and VBScript malware analysis, and a session on the theoretical and practical implications of supervised automation of malware variant generation. A live memory forensics tutorial also proved to be worth the visit.

The real meat of the conference itself began with an opening word from the chairman of EICAR, Rainer Fahs, followed by a keynote address from Professor Dr Fred Cohen. The professor is widely acknowledged as having been the first person to define the term ‘computer virus’, having included the definition in his 1984 thesis. He is also the author of the Deception Toolkit – well known today in the UNIX/*Linux* world. Prof. Cohen’s speech – which was an absolute highlight – gave a nice indication of the differences between commercial and academic views of the malware problem. He concluded that viral computing is here to stay, and that we have to live with it, but that we really must put thought and effort into defending ‘our’ cyberspace and the very vulnerable infrastructure behind it.

After Prof. Cohen’s speech, Ronald Schulze from *BDK* described a project called Webpatrol – an interesting approach to handling Internet emergencies by using feedback forms filled in by ordinary users. Boris Sharov from *Dr. Web* continued the morning’s presentations with an excellent overview of some newly detected malware. After this, the conference split into two tracks with a mixture of industry and academic papers – which makes this conference quite unique these days. As always, it was hard to decide which stream to follow.

First, I attended a presentation by Magnus Kalkuhl from *Kaspersky Lab*’s Global Research Team, who described some of the undesirable situations that could potentially arise in the next 10 years. The more people depend on computers and robotics, the stronger the impact that malware will have on their lives – not only in financial terms, but with serious consequences for victims’ lives. Magnus looked at some of the ways in which the risk could be reduced, which seemed a bit utopian at first, but that might have been due to their futuristic nature. This was a real science fiction thriller.

And there was more to come: Babu Nath Giri from *McAfee* presented a paper entitled 'Malware in men'. By combining materials from two studies he demonstrated that implantable medical devices are vulnerable to malicious attacks. He discussed the possibility of such malware arising in the future. I must confess that, after hearing what Babu had to say, I would think twice before having a bionic eye or a hearing aid implant!

Another enjoyable presentation from *McAfee* (by Ramagopal Prashanth, Mohandas Rahul and Thomas Vinoo) was about the rise of autorun-based malware. The paper looked at advancements in this type of malware. Thomas discussed methods that can be used proactively to detect and stop malware that spreads via removable drives, using a combination of traditional anti-virus and cloud computing techniques. Later, Michael Friela's presentation detailing his risk behaviour index gave an insight as to how the use of psychology in the context of security could help create awareness by changing human behaviour. Such a feat is easier said than done, and I have my doubts about its viability, but remain open minded.

That evening, the conference gala dinner provided an opportunity to relax and enjoy a real treat: magician Didi Saxer put on a perfect show with a brilliant mixture of comedy and magic.

The following morning, Professor Dr Nikolaus Forgo presented an overview of the current status of and recent developments in European legislation on data protection and data security. Of course, Prof. Forgo's presentation touched on the topic of the possible German 'BundesTrojan' and the issues that it raises for the security industry. EICAR will continue to monitor legal developments in Europe as they become increasingly important.

For the first time in the history of the EICAR conference, the best paper prize was awarded to an industry paper which brilliantly combined elegant theory with practical applications in critical fields: Sébastien Tricaud and Philippe Saadé's 'Applied parallel coordinates for logs and network traffic analysis'. If you are mathematically minded this paper is a must-read.

One of the specific areas this EICAR conference focused on was anti-malware testing. David Harley and Randy Abrams from *ESET* presented a paper on 'Execution context in anti-malware testing'. They reviewed the most common mainstream anti-malware detection techniques and tried to clarify the terminology most commonly used in this context in relation to the technology it describes. Hopefully the attempts by AMTSO to establish testing standards, and anticipated parallel initiatives from EICAR, will start to break down psychosocial barriers to the popular acceptance of the need for more rigorous testing practices.

Other papers on the subject of testing included an empirical evaluation of whether behavioural anti-virus products are able to detect complex metamorphic malware (Jean-Marie Borello, Ludovic Mé and Eric Filiol from ESIEA); a paper entitled 'Applied evaluation methodology for AV software' (Alexandre Gazet and Jean-Baptiste Bédrune from Sogeti/ESEC); and a study of 'anti-virus response to unknown threats' (Christophe Devine and Nicolas Richaud from *Thales Security Systems*), which gave some insight into problems relating to anti-malware products. My advice to some of the authors is to take a deeper look at the AMTSO documents – however, from a theoretical point of view, the papers were quite interesting.

Andrew Hayter from *ICSA Labs* looked at how the accreditation of testing and certification programmes under the ISO 9001 and 17025 standards could provide assurance both to the anti-malware developers and to the endpoint consumer that test labs meet the rigorous standards set by the International Standards Organization. Meanwhile, Ferenc Leitold from *Veszprog* described a unique and closed testing and certification procedure that could be used for dynamic testing.

A good part of both the commercial and academic anti-malware worlds were represented in a panel session about anti-malware testing, which was another highlight of the conference. This session continued to provide a deeper look at and better understanding of the principles of testing and the complexity of the issue. It was agreed that we need recognized testing standards and some independent body(ies) to regulate testing, all for the benefit of the user. This is also the approach of the AMTSO initiative. In determining these standards and regulations we should include as many organizations, vendors, academics and testing bodies as possible, but we must not forget also to include the end-users.

By the time you read this, or soon after, most of the presentations from this year's conference (including those I have been unable to include in this summary) will be available on the EICAR conference website (http://www.eicar.org). This year saw a significant increase in both the quality and quantity of papers submitted for the conference, and the event itself was a great success.

The 19th EICAR is due to take place next year in France, at the ESAT facilities (Ecole Supérieure et d' Application des Transmissions) in the heart of Paris from 8 to 11 May 2010. A call for papers as well as more detailed information will be published soon. Mark the dates in your diaries!