CONFERENCE REPORT

EICAR 2010: RAINY DAYS IN PARIS

Eddy Willems
G Data Software and EICAR, Belgium

The 19th EICAR conference took place last month in the heart of the beautiful city of Paris at the Ecole Supérieure d'Informatique, Electronique, Automatique (ESIEA).

Paris in the sunshine.

The second International Alternative Workshop on Aggressive Computing and Security (iAWACS'10) was held immediately before the conference at the same venue, and EICAR delegates were also able to attend this event. iAWACS'10 included workshops on smart cards and crash courses on securing PLC networks, but the most noteworthy item on the agenda was the anti-virus evaluation challenge 'PWN2KILL', the aim of which was to attempt to bypass anti-virus software and evaluate its effectiveness in practical terms. A technical summary is available on the iAWACS website. [*David Harley shares his views on the challenge on p.2 – Ed.*]

GETTING STARTED

After an official EICAR members meeting and welcome party on the Sunday evening, the real meat of the conference began on Monday morning with an opening address from the chairman of EICAR, Rainer Fahs, continuing with a keynote from Christophe Devine – better known as the father of 'Aircrack' – about problems related to AV testing. He described a series of tests and rated their usefulness. Devine believes that, in most cases, careful inspection reveals no real winners, and several tests are not even relevant to the real world. He proposed an initiative called AVerify, an open-source anti-virus test suite which would facilitate the creation of reproducible, more reliable tests. AVerify would be inspired by the EICAR test file, maintained independently of EICAR but following the same code of conduct.

'Parasitics, the next generation' was a joint paper from Vitaly Zaytsev (*McAfee*) and Josh Philips (*Kaspersky Lab*), in which an in-depth analysis of two of the most recent advanced and sophisticated viruses (W32/Xpaj and W32/Winemem) was presented along with the new techniques they use to transform their code to avoid detection. Zaytsev and Philips discussed ways in which VM-based obfuscators can be defeated.

Zdenek Breitenbacher used 'Lego building blocks' to demonstrate that although each copy of polymorphic malware is totally different in a simple binary view, we can still find some characteristics that always remain more or less the same. He discussed a characteristic the malware analyst can use: entropy. But instead of calculating the entropy as a single number describing the whole file, we need a very detailed map which plots entropy throughout the file. He showed that by inspecting the entropy map, a malware analyst can easily isolate the innocent and the suspicious parts of the file. The entropy map of one polymorphic family often remains the same for all of its copies. In fact, such an entropy map can act as a special kind of signature, which could be used in the same way as a traditional signature. The entropy map offers a new and unexpected view of malicious files and may help malware analysts in many different tasks.

Igor Muttik revealed 'a single metric for evaluating a security product'. He analysed the factors contributing to the probability of successful protection, presented a mathematical approach to calculating this probability and discussed how this can be implemented in practice. He showed some examples of how the growing frequency of attacks dictates a statistical approach to measuring the quality of security software. Lysa Myers from *West Coast Labs* gave us an insight into their new testing techniques, and Alexey Tkachenko from *Dr. Web* presented a detailed analysis of the nasty Backdoor.Tdss rootkit (aka TDL3).

That evening the conference gala dinner provided an opportunity to relax and enjoy good French food and champagne during a pleasant boat trip on the river Seine. While heavy rain disrupted a short walk by the river, the beautiful sparkling lights of the Eifel tower in the background created a truly magical atmosphere.

BEST PAPER

For the first time in the history of the EICAR conference, the best paper prize was awarded this year to an industry paper which combined elegant theory with practical applications. In her paper 'Symbian worm Yxes: towards mobile botnets?', Axelle Aprvrille described how this mobile malware connects to the Internet, installs new malware or spreads to other victims. She explained how malicious remote servers participate in the configuration and propagation of the malware, noting Yxes's similarities with a botnet. The paper shows the importance and lack of

Paris (and delegates) in the rain.

security on mobile phones. It also indicates several areas on which future work should focus, such as communication decryption and tools to analyse mobile-embedded malware.

Jan Vrabec and David Harley shared their views on the methodology and categories used in performance testing of anti-malware products. This seems to remain a contentious area. While there is plenty of information on detection testing, very little is available on performance testing. The paper aims to objectively evaluate the most common performance evaluation metrics used in anti-malware testing, such as scanning speed, memory consumption and boot speed, and to highlight the main potential pitfalls of such testing procedures. Vrabec and Harley made some recommendations on how to test objectively and how to spot potential bias. A nice paper, and a must-read!

'Crowdsourcing' is best defined as 'a neologism for the act of taking tasks traditionally performed by an employee or a contractor, and outsourcing them to a group (crowd) of people or community in the form of an open call'. In her paper, Methusula Cebrian Ferrer posed the question of whether there could be a future for crowdsourcing security. As web-based technologies move towards interactive social media, real-time web, and capturing geo-specific content, it is important to understand whether crowdsourcing could be a viable strategy for the security industry. In other words, collective security intelligence is becoming a necessity if we want to deal with the amount of data which besets us: the problem is that this is easier said than done.

In 'Perception, security and worms in the Apple', David Harley, Pierre-Marc Bureau and Andrew Lee compared the view from *Apple* and its user community as a whole with the view from the anti-virus labs of the actual threat landscape. They examined the ways in which the *Apple*-using community is receiving increasing attention as a potential source of illegitimate profit, reviewing the directions likely to be taken by malware over the next year or two, and assessing the likely impact of attacks against *Apple* users and the implications for business and for the security industry. As the Mac user community still sees the Mac as a safe haven, it is indisputable that this platform will see many more problems arise in the future.

Vlasti Broucek from the University of Tasmania discussed 'the cost of university Internet access' and highlighted the need for continued vigilance on the part of users, network administrators, service providers and policy makers. Using examples from two different areas of the university, he demonstrated, that if we are not to create an Internet of 'Big Brother surveillance', or even worse one of 'self-censoring behaviours' – or force mass adoption of encryption to ensure privacy and the security of users from prying eyes – then user education, change management and communication from the very top right to the bottom of the organization will play a vital role.

AND FINALLY

The final paper on the programme was a very interesting theoretical and academic paper presented by four ESIEA students (Jonathan Dechau *et al.*), who attempted to evaluate the ability of anti-virus to detect malware spreading through *Office* documents. The paper used the EICAR test file to demonstrate that macro-based attacks are very easy to put into action, and prompted some heated discussions about problems related to signature-based detection. Some of the paper's conclusions were potentially flawed, having been based on non-detection of modified versions of the EICAR test file (see p.2). However, the theory behind this research seems to be perfectly correct and will inspire more discussion about the detection methodologies currently used and the consequent problems in all security products these days: this was, of course, the real message behind the presentation.

LOOKING BACK AND LOOKING AHEAD

By the time you read this, or soon after, most of the presentations from this year's conference, including those I've been unable to include in this summary, will be available at http://www.eicar.org/. Once again this year saw a significant increase in the quality and quantity of papers submitted for the conference and the event itself was a great success. As one of the founding members of EICAR, I remember the first constitutional conference in Brussels in 1991. A lot has happened and improved during those 19 years and I fully expect this to continue. The location of the 20th EICAR conference has yet to be decided, although rumours are spreading quickly. A call for papers and announcement of dates and venue will be published soon.