



EICAR 2010: ICT Security – Quo Vadis? Overview of the conference: why to attend EICAR 2010?

The 19th EICAR (European Institute in Computer Antivirus Research) conference will take place in Paris from May 8th to May 11th including a pre-conference program that should be a milestone in the history of computer antivirus research. In fact the whole conference itself is intended also to be a major event in the field and thus for many reasons.

The AV world -- and more widely the computer security world-- is facing for a few years big challenges. BUT contrary to partially wrong feelings those challenges are not only coming from the bad guys: usually all those ugly actors who think to be intelligent or having some sort of power by distributing malware. While all the instances (the defenders, e.g. AV vendors, governments, researchers, IT experts...) involved in fighting those malevolent guys (the attackers), the motivations has begun to diverge substantially for a few months, in such a way that it not only becomes more difficult to make the difference between defenders and attackers but also finally the result is that the activity of the attackers is made easier: here precisely lie the new challenges that the EICAR 2010 has decided to address. Hence the main theme of the event: **ICT Security – Quo Vadis?** I would be tempting to use an equivalent formula: is the AV world and the ICT world going mad? Let us see why through two illustrative but worrying recent issues.

The first one refers to AV evaluation – which will be addressed at EICAR 2010 as a one of the major topics. The situation is somehow worsening making that evaluation, from an independent, technical perspective more and more difficult not only from a technical point of view but also from a legal point of view. To realise how things are evolving, anyone can read any AV software licence document (the one which nobody reads in fact): you will discover, according to the product, in a jumble that you cannot use the product in any automated way (which is quite limiting in a context of black box evaluation), you cannot even analyse the product, you are warned that your data can go outside for analysis (but where), that the encryption embedded in the product is weak on purpose in order to facilitate US governmental decryption... Is it really serious and does it take the needs and interest of the end-user which are not simple "consumers". In this respect, the reaction of the AV community goes in the wrong direction and is perceived as just trying for 20 years more just to protect their commercial interest. On the contrary it should work deeply and in a trustful way with the scientific community. Nobody has the right to forget that there is ONLY one target: malware and those who spread them. The recent evolution of the use of cryptographic primitives into malware (remember Confiker), the rise of metamorphic like techniques require now that all good wills work together. That is why EICAR 2010 will focus on the evaluation of AV software, in such a way that we provide a useful reflexion for better products while taking into account the end-users needs, the ethical and legal aspects and the scientific/technical challenges we are bound to face in a very near future. Aside the classical academic and industry papers which will be presented, the two-day preconference program will propose tutorials, student/industry sessions around the topic of AV software and AV policy evaluation. Especially, we intend to offer and promote new tools and tutorials with respect to them, that everyone could use to evaluate himself his own AV security and policy. It will be the occasion to recall that the only independent way to test an AV without using any malware – a critical issue in itself – was, and still is, the EICAR test file. We will propose,



especially for the industry, a tutorial on that file and on new open forthcoming tools that will be disclosed and presented during EICAR 2010. Those tools are directly inspired by the EICAR test file but go far ahead to address the new challenges and needs. So it should be a good reason to attend the conference.

The second case is the very worrying evolution of the use of malware for so-called "investigation" and "copyright protection" purposes. A number of countries (USA, Germany, UK, France, Austria, Switzerland, have officially announced that malware-like technologies (e.g. Trojan horses for the most part) are now authorized to enforce the law. More worrying is the use for commercial purposes (as it is the case when trying to monitor users' downloading in order to fight piracy). The question is: is the remedy not worse than the disease? Such issues should be addressed at the EICAR 2010 conference. BUT the main consequence of that evolution lies in the way the AV community will react and what it will decide: either AV vendors accept not to detect those malware-like technologies (which is bound to be very difficult from a behavioural detection point of view, unless closely collaborating with the governments) or they refuse and will detect them anyway. Well, it reminds us the critical issue of the FBI Trojan horse Magic Lantern, except that now we have a lot of Magic Lantern codes which are about to be used. If the AV community chooses the first solution – to cooperate with the governments – they are going to lose their credibility and legitimacy very quickly, making precisely the game of the bad guys. Why? Because they implicitly would accept the fact that there is such things as good and bad Trojan Horses. What is quite impossible to manage from a technical point of view, would be a nightmare from a legal/society/privacy point of view. In fact, they are just about to open the Pandora box? That is the reason why we have decided at EICAR 2010 to also address these kinds of topics. The ICT world has now invaded our society and personal lives and we cannot remain blind to its evolution.

I would like to quote Francois Rabelais, a famous French writer, from the 16th Century: "**Science without conscience is the soul's perdition**". It could be the EICAR 2010's motto. So you now know why you must attend the conference. Look for the EICAR website. More details will be published by mid September. You can also register to the EICAR forum where you will find a lot of useful information.

Professor Eric FILIOL
EICAR Scientific director
EICAR 2010 Program Chair
dirscience@eicar.org