



'Crossing over to the Dark Side of the customer/vendor divide has made me increasingly aware of just how bad "bad" can be.'

David Harley, ESET

PWN2KILL, EICAR AND AV: SCIENTIFIC AND PRAGMATIC RESEARCH

I guess no one joins the anti-malware industry for a peaceful working environment, a celebrity lifestyle, or a need to be loved by the world in general and other security professionals in particular. (If they do, they probably move quickly on to a role with a more congenial working environment, such as traffic warden, flak jacket model, or leader of the Labour Party.) And while I've visited the topic of AV's bad reputation before (see *VB*, November 2006, p.6), crossing over to the Dark Side of the customer/vendor divide (my name is David, but you can call me Darth) has made me increasingly aware of just how bad 'bad' can be.

At the first International Alternative Workshop on Aggressive Computing and Security (iAWACS), held in 2009 by the École Supérieure d'Informatique, Electronique, Automatique (ESIEA), a 'PWN2RM' challenge was held, in which a number of anti-malware products were installed on a machine and attempts were made (while logged in as administrator) to disable them. The attempts were successful in most cases (see <http://www.esiea-recherche.eu/data/pwn2rm.pdf>.) An interesting idea, and though a compromise with physical access and administrator privileges doesn't necessarily

translate easily into an automated malware attack, and still less into a meaningful metric for ranking products, the disabling of security processes is a very common feature of malware attacks.

At the second workshop, held last month, the 'PWN2KILL' challenge took the idea several steps further. The rules of the contest stated that its aim was to perform a 'comparative evaluation of commercial anti-virus software', using a variety of attacks. The slides relating to the 2010 challenge are available at ESIEA's website, and the number of vendor fails recorded is pretty worrying. The technical briefings for some of the attacks are very sparse on detail, so I guess the vendor community will have to wait until the attack code becomes available before we can fully evaluate and learn from the challenge.

Until then, it would be premature to sound the death knell of anti-malware on the basis of this challenge. Scientific method is a Good Thing, but it doesn't matter whether the methodology is reproducible if it isn't right. A paper presented by Dechau *et al.* at last month's EICAR conference focused on one of the attacks used in PWN2KILL and inspired heated discussion among delegates. Defensibly enough, the students were restricted to attack code that was based on attempting to bypass anti-virus in order to execute the EICAR test file. However, that particular combination of methodology and sample created problems, since some of the paper's conclusions were based on non-detection of modified versions of the EICAR test file – in violation of the test file's specifications (see *VB*, June 2003, p.13 and EICAR's own description). Vendors were understandably disturbed at being penalized for conforming strictly to the specifications. Nonetheless, it would be a pity to focus on that hiccup rather than on the message behind the presentation, as voiced with passion by EISEA's Eric Filiol and EICAR chairman Rainer Fahs.

They're not alone in their disappointment that anti-malware products cannot provide anything like 100% detection and resistance to attacks. As researchers, we can argue that we have never claimed that anti-virus kills 100% of malware, let alone other attacks; that we (largely) abandoned signature detection for algorithmic methods years ago; that we've long advocated multi-layered defence; and that a business cannot survive on R&D without marketing. But we need to understand the insights and needs of academics and customers with critical systems, just as they need to understand our need to deliver pragmatic, market-driven solutions.

In the meantime, I'm considering changing my name from Darth to Aunt Sally.

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Consulting Editors:

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, USA*