EDITORIAL

I say Virus, You say Trojan

The basis of any successful information exchange is the common understanding of the language used by all parties involved. As long as we all know that while 'I say tomato, you say tomato', we are still talking about the same thing, and we can have a fruitful discussion. However, if you mention bananas and I start discussing 'ananas' ('pineapple' in many European languages), we will soon be in deep trouble. If we don't figure out quickly that we are talking about different things, our dialogue will become the source of confusion and doubts in each other's mental abilities.

"how do we classify the code to define its nature?"

Most new technology, especially in computer and programming terms, reflects the considerable effort of rendering new inventions and discoveries more comprehensible by naming them after existing, well-known objects or subjects with analogical features/behaviour. While some analogies are obvious (few cannot yet distinguish a hard disk from a floppy), most terms, recognizable in inner circles, are meaningless to outsiders. For those not involved in Electronics, a 'floating gate' might have more in common with a sluice than a computer.

The biological analogy of the term 'virus' reflects similarities in the behaviour of computer and biological viruses perfectly. It also acts as an intuitive aid to understanding the nature of computer viruses. The term 'trojan' is commonly used by the anti-virus and computer security industries to specify a certain type of malicious software. To 'outsiders' though, it would sound more like a contraceptive product and, to historians in particular, it is likely to conjure up visions of the wooden horse the Greeks built while besieging Troy (from which the analogy derives). The idea of 'a worm' crawling through one's machine usually beats the imagination of an average PC user.

The anti-virus industry has been doing its best to increase awareness of virus threats. In a way, it has been successful – now, if anything goes wrong, the first thing people look for is a virus. Virus detection and removal is perceived by some users as a very clever, almost magical process, but there is no reason a magician shouldn't do easy tricks as well as difficult ones. If you are a 'good guy', tracking and fighting thousands of viruses, why don't you fix some silly, non-replicating trojans, worms, jokes and corrupted files? If trojans seem to be more dangerous than viruses, why don't anti-virus vendors tackle those too?

Because they argue that, by definition, they develop anti-virus, not anti-trojan or anti-malware, software. Some try to meet demand by including in their products the detection of trojans and jokes. At this stage, users should be able to have a clear picture of who's detecting what. Of course, this is assuming that everyone involved in anti-virus research knows how to classify code and agrees on what a virus is, what a trojan is… etc. Unfortunately (or not,) complexity is the essence of the universe; the world (including that of viruses) is not black and white with borders clearly and forever defined. The more we know about viruses and other malicious software and the greater the diversity of ideas and tricks implemented, the more valid are the arguments for new classification and naming schemes. There is a strong desire to do things right and not to compromise one's principles – this is often the position of anti-virus researchers. Sometimes, however, adhering to these priciples makes it difficult to provide the clear answers and simple solutions that users prefer.

The latest and one of the longest such discussions (two months to date) has centred on the classification of so-called AOL trojans. There are more than enough reasons to categorize at least some of them as viruses, but at the same time, there are legitimate arguments to classify them as trojans or even worms (based on respective definitions). All agree, however, that it is unwise to misname these programs for the convenience of either the anti-virus community or users, but how do we classify the code to define its nature? The worst possible outcome is to assign the multiple label 'trojan virus' or 'virus trojan'. This is not only confusing, but contrary to current standards. Whatever the outcome, this will always be a controversial entry in the anti-virus dictionary. This is not the first and certainly will not be the last case of its kind.

Jakub Kaminski, Technical Editor

VIRUS BULLETIN **©1998 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /98/$0.00+2.50**