FEATURE

CARO: A Personal View

Fridrik Skulason

The past five years have seen many attempts at forming anti-virus organisations. I have watched them come and go, and seen many replaced by other groups with slightly different goals. Often, however, ‘core’ participants remain the same - the number of people in this field is rather limited.

One organisation was *AMC* (*Anti-virus Method Congress*), a short-lived attempt to unite developers and users which fell apart the day it was formed. Then came *VSI* (*Virus Security Institute*), an organisation of researchers and developers which attempted (and failed) to hold a virus conference - and is now reduced to an almost inactive mailing list.

AVPD (*Anti-Virus Product Developers*) was, as its name indicates, an organisation of companies within the industry. It may still exist - I personally lost interest in the group some time ago. Others include *NCSA* (*National Computer Security Association*), *ICSA* (*International Computer Security Association*), *CVIA* (*Computer Virus Industry Association*) and *EICAR* (*European Institute of Computer Anti-virus Research*). Some still function: not all are limited to computer viruses; some deal with security in general.

There is an organisation of *Macintosh* virus experts, which seems to be trying to keep its very existence, or at least its members’ names, secret. Finally, there is *CARO* (*Computer Anti-virus Research Organisation*). These last two bodies are different from those mentioned above, actually doing things to benefit their members, and, indirectly, the whole user community. I will not attempt to describe the *Macintosh* organisation, but as a founding member of *CARO*, I should be qualified to explain what *CARO* is - and is not.

CARO: The Beer-Drinking Club

CARO members have always made it clear that the group is not an industry association. It might best be defined as an informal organisation of people (*CAROts*) who get together every now and then, drink beer, eat pistachios, try Chinese restaurants all over the world (ever wondered why some of us are slightly overweight?), and chat about such subjects as computer viruses and uses of leftover military hardware. Between beers, *CAROts* exchange virus information, or even live samples.

CAROts live in every corner of the globe, and can rarely sit down together, so we frequently correspond by Email. *CARO* is not officially registered anywhere and has no membership fees, no formal charter of operation, minimal overheads: exactly how it should be. The most formal organisations in this area have also been the most short-lived, and the worst waste of time for all involved.

An Organisation of Individuals

CARO is an organisation, not of companies or company representatives, but of anti-virus authors and researchers, some of whom work for companies producing anti-virus soft- and hardware. In some cases this distinction does not matter. Some members run (or used to run) a single-man company; others work for companies with huge legal departments (it would be more difficult for such people to join as official company representatives than as individuals).

If a *CARO* member switched companies, he would almost certainly remain a member, the company he left having no right to appoint a ‘replacement’. In fact, *CARO* participation is not always actively supported by companies for whom members work - marketing departments do not always seem to like the idea of their technical people meeting with the competition over a glass of beer (many glasses, in fact…). Other *CAROts* do not work for anti-virus companies at all; for example, those at universities.

CARO Activities

Ignoring the beer-drinking and other activities which have nothing to do with viruses, *CARO* activity falls into one of five categories: virus-naming, virus descriptions, the *CARO* WildList, exchange of viruses (or virus information), and the *CARO* mailing list. Many of these benefit, at least indirectly, the user community.

Within *CARO*, a small naming committee (Alan Solomon, Vesselin Bontchev and myself) is responsible for selecting ‘official’ names for new viruses. *CARO* has no power to force anti-virus companies to adopt these names, but we do our best to encourage it: this would help to reduce the confusion caused by the use of multiple names for one virus.

There has also been work on a database of virus descriptions, called *CaroBase*. This is intended to provide a more accurate alternative to *VSUM*, but has not yet reached distribution stage. If and when it does, the benefits will be obvious - there is a need for an extensive, accurate virus information database.

The WildList is (just as the name suggests) a list of viruses ‘in the wild’, kept up to date by Joe Wells, who works for *Symantec*. It collates reliable reports from all over the world on virus frequency and incidents. It cannot be 100% accurate, but is the best list of its kind currently available.

When *CAROts* meet, they may exchange recently-received viruses and various bits of virus-related information. Meeting in person often involves setting up a small LAN: one *CAROt* brings a portable *NetWare* server and the rest bring laptops, adapters, T-pieces and short cables. Everyone participating uploads his material, and downloads the rest.

There are several mailing lists for use by *CARO* members, for technical purposes. These are closed to non-members, but one (vquery@rz.uni-karlsruhe.de) enables interested parties outside *CARO* to send queries to members.

The *CARO* Collection

One often hears about this: sometimes a computer magazine will request access to it, and there have been cases of someone claiming to have obtained it. However, the truth is that there is no such thing as a *CARO* virus collection. Most members maintain their own collections, and although they may be similar, they are certainly not identical. Of course, some are bigger or better organised than others - the best collection is probably that of Vesselin Bontchev in Hamburg, but even this cannot be called 'The *CARO* Collection'.

Joining CARO

When *CARO* was formed on 10 December 1990, there were fewer than ten members, but today there are nearly 30 *CAROts*. Joining *CARO* is not a simple matter of signing a form and paying a membership fee. Some new members are invited; others apply and pass the voting process. Existing *CAROts* vote on candidates, and each member has the right to veto any application. Even if nobody rejects a candidate, a certain percentage of members must actually vote for him, instead of abstaining.

Does this sound harsh? Maybe, but keep in mind that *CARO* is not an industry association which does not care who the members are, as long as they pay their annual membership fee. This is a group of individuals who trust each other, and who must be able to do so: we regularly exchange sensitive information which we want to prevent falling into the wrong hands. Although this does not imply that members have to like each other, it is usually the case that we do.

An application may be rejected for several reasons, but some are more common then others. For example, the 'Who's that?' problem: there have been a few cases where applications were received from people few *CAROts* knew personally or with whom they had corresponded. Such applications generally failed because too many *CAROts* abstained.

Any application from known virus authors, anyone involved in unrestricted virus distribution, encouraging virus writing or behaviour considered unethical by *CARO* members will be rejected without consideration. In addition, we expect a certain level of viral knowledge, as well as several years' experience in the field. Applications from those interested only in collecting viruses are rejected immediately.

There have been occasional accusations that this makes us an 'elitist' club… there may be a grain of truth in that, but this system has kept *CARO* working for several years, and enabled us to get some useful work done, as well as having great fun between glasses of beer. [*The next CARO meeting is planned for the VB Conference in Jersey. The bar has already been informed. Ed.*]