

## BOOK REVIEW 1

### THE ART OF DEFENCE

Vanja Svajcer  
SophosLabs, UK

**Title:** The Art of Computer Virus Research and Defense  
**Author:** Péter Ször  
**Publisher:** Addison Wesley for Symantec Press  
**ISBN:** 0-321-30454-3

It has been more than six years since I started working as a virus researcher, but I remember the first few months vividly. The beginning of any job is difficult, but even more so if you have to acquire your skills using a number of highly scattered, incomplete and sometimes suspicious resources.



As a beginner, I was surprised and disappointed to find out that there were very few books on the subject of computer viruses. Furthermore, none of the books were dedicated to people who, like me, were eager to dig into the low-level technical issues of viruses and the technology required to tackle them. Some books, like Fred Cohen's *A Short Course on Computer Viruses*, were intriguing but I felt I needed something more practical – a proper handbook to point me in the right direction. Unfortunately, for me, there was no choice but to learn the hard way.

It was with great excitement, therefore, that I learned recently that Péter Ször's book *The Art of Computer Virus Research and Defense* was to be published. I pre-ordered a copy straight away and waited for what seemed like forever to receive it.

Although I had not known what to expect, my first encounter with the book reassured me that I would not be disappointed. The book weighs in at 675 pages and is the result of one year's work – which is even more impressive considering the fact that it was written mainly during weekends. Behind the book's impressive content is not just Péter's 15-plus years of expertise, but also a breadth of knowledge gathered from many of the best-known members of the anti-virus research community.

The book is divided into two parts and 16 chapters. The two parts, 'Strategies of Attacker' and 'Strategies of Defender', are dedicated to a specific set of problems but there are many occasions where this division blurs. The title 'Strategies of Attacker' may sound a little confusing, but the content is always written from the point of view of a defender and very few ideas are exposed that could be used by a malicious reader. At the end of every chapter is a very useful list of references for those who need to know more.

The introductory chapters are clear and well structured, but I felt that they could have been a little gentler for beginners. Although the book states that the reader is expected to have a programming background, a chapter containing an introduction to the CPU architecture, assembly language and operating system would have been a beneficial addition for the less experienced reader – without this, some of the early assembler examples could prove discouraging.

The first part of the book shines as this is where we find Péter's best known work – the technical details on Win32 threats, vulnerabilities and exploits, worm analysis and particularly interesting coverage of polymorphism and metamorphism. This part of the book is the most valuable to any reader who is keen to learn as much as possible about current viral threats and the technology used by the virus-writing community. Here the majority of content is derived from articles published in *Virus Bulletin* or papers presented at various conferences. It is certainly a good thing to find all that work in one place but I felt that in some cases the otherwise natural flow of the book was interrupted.

The second part of the book is a pleasant surprise and demonstrates Péter's intimate knowledge of the internals of many anti-virus and security products and technologies. This part of the book is an excellent source of information when one needs to explain the fact that modern anti-virus software uses a set of increasingly sophisticated methods for virus detection. The chapter containing an introduction to anti-virus technology is followed by detailed explanations of problems and solutions for handling *Windows* memory scanning and disinfection, as well as deep insights into generic blocking techniques and network level defence.

The 'Strategies of Defender' section contains a very useful chapter on analysis techniques. The chapter also gives an overview on how to set up a virus analysis laboratory. Although the book provides a good level of detail I felt that this subject should span more than one chapter. One would guess that time constraints prevented further coverage of this subject, and hope that the content will be expanded in the next edition(s). Another useful addition to the book would be a CD-ROM containing the tools used to analyse viruses and perhaps some demonstration programs that the reader could use to practise the analysis.

My only objection concerns the title of the book, which suggest that its scope is as majestic as Knuth's *The Art of Computer Programming*. Even with twice as many pages and double the content the book would not be able to reach the depth required to describe the subject fully. For me, a better title would have been 'An Overview of the Art of Computer Virus Research and Defense'. However, this does not prevent Péter's book from being, in my opinion, the best book on the subject published to date.