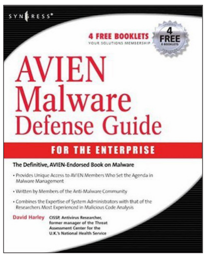
BOOK REVIEW

BIRDS OF A FEATHER...

Martin Overton
Independent researcher, UK



Title: AVIEN Malware Defense Guide for the Enterprise

Author: David Harley, *et al.*

Publisher: Syngress

ISBN 13: 978-1-59749-164-8

Pages: 540

Cover price: $59.95

The *AVIEN Malware Defense Guide* has been written by members of the AVIEN/AVIEWS online communities with the aim of passing on knowledge that they believe will be both interesting and useful to those involved in the real-world battle against malware in organizations.

The cover of the book claims that it will 'stop the stalkers on your desktop' and also provide:

- Complete coverage of the relationship between enterprise security professionals, customers, vendors and researchers.
- In-depth consideration of key areas of the 21st century threat landscape.
- System security and DIY defence using a range of specialist detection and forensic techniques and tools.

Meanwhile, the back cover states: 'AVIEN members represent the best-protected large organizations in the world, and millions of users. When they talk, security vendors listen: so should you.' So, after making such a bold statement, does the book deliver on the promises it makes?

UNDER THE COVERS

The book contains 11 main chapters and two appendices. It starts with a short biography of each of the contributors, before moving on to a very brief foreword, penned by Robert Vibert, who was administrator for AVIEN at the time the book was written.

This is followed by a preface and introduction, both written by the book's main author David Harley, in which an overview of each chapter is provided in a concise, but friendly manner.

CHAPTER AND VERSE

The start of each new chapter is marked by a cover page which presents a list detailing the content of the chapter. The publisher calls this list 'Solutions in this chapter' – even when the subject matter of the chapter relates to threats, rather than solutions. Every chapter concludes with a 'Summary', a 'Solutions Fast Track' and a 'Frequently Asked Questions' section.

Chapter 1, 'Customer power and AV wannabes?', is a nice gentle introduction, describing how AVIEN and AVIEWS started and how they have evolved over the years. It moves on to discuss how the anti-virus industry reacted, initially with some suspicion, to the formation of the groups, before realizing that AVIEN wasn't a vendor-bashing forum but a valuable information-sharing resource.

The reader is then asked 'So you want to be a bona fide computer anti-malware researcher?', which is followed by 'You should be certified' (not *that* sort of certified, even if eccentricity does seem to be a common trait in the industry), and the chapter finishes off by considering the question 'Should there be a vendor-independent malware specialist certification?'.

Chapter 2, 'Stalkers on your desktop', ups the pace a little by covering malware nomenclature – this is always a fun topic as vendors rarely agree on naming (in theory, yes, in practice, no). The chapter covers the CARO naming convention, as well as the Common Malware Enumeration effort led by *MITRE*. We then take a trip down memory lane with a look at the birth of malware. Viruses, trojans and worms are covered, as well as spam, rootkits and scams, and finally hoaxes and chain letters get the once over.

Chapter 3 is entitled 'A tangled web' and covers the threats that rely on HTTP, such as index hijacking and hacking into websites. It moves on to discuss browser vulnerabilities and attacks on DNS servers, such as DNS poisoning (pharming).

After looking at the threats the chapter turns its attention to some of the many solutions available as well as the testing of HTTP-scanning solutions, and covers 'malware and the web: what, where, and how to scan' and 'parsing and emulating HTML'. It also covers some of the legal issues associated with the business of blocking malicious threats from the Internet, looking specifically at patents and the all too common litigation between patent holders and anti-virus companies.

Chapter 4 is entitled 'Big bad botnets' and is essentially a compressed version of several chapters of another recent *Syngress* book on botnets (see *VB*, June 2007, p.7).

Chapter 5, 'Crème de la cybercrime', covers the changing face and motivation of malware authors, looking at both old-school virus writing as well as the more recent developments of the blackhat economy.

This is underlined by a couple of case studies which clearly show the current motivation of the bad guys involved in malware authoring and cybercrime. The chapter finishes off with a look into a virtual crystal ball and discusses what won't change, as well as the things that are more likely to happen. These include not only techniques such as social engineering, but also technologies, such as VoIP, credit cards and podcasts.

Chapter 6 is entitled 'Defense-in-depth' and describes the technique very thoroughly, explaining what it is and how to implement it. More importantly it also covers some of the areas that often get forgotten and even goes as far as covering malware laboratory procedures. For most corporate security personnel, this chapter will be indispensable. It is a real goldmine of useful material and very well thought out.

Chapter 7, entitled 'Perilous outsorcery', covers the thorny and emotive subject of outsourcing anti-virus services. It not only covers how outsourcing can best be achieved, but also some common mistakes and the importance of two-way communication.

The key thing that is made absolutely crystal clear in this chapter is that outsourcing anti-virus services is not a quick fix, even if your existing in-house anti-virus service isn't broken or badly sprained before you decide to pass this 'hot-potato' to your chosen outsourcer. I couldn't agree more.

Chapter 8 is entitled 'Education in education' and, not surprisingly, covers the subject of user education. However, it discusses it in a new and refreshing way, looking not only at the subject from an educationalist's perspective, but also the issue of security in education.

The chapter concludes with 'Not exactly a case study: the Julie Amero affair'– discussion of a contentious court case in the USA that has been hot news in the anti-malware industry since the story originally broke in January this year. The whole chapter is very well written and extremely well thought out.

Chapter 9, 'DIY malware analysis', is the most technical chapter in the book as it deals not only with analysing malware using web-based tools, but also using debuggers and disassemblers for static code analysis. It also covers, in some depth, dynamic analysis in virtual environments such as *VMWare* and *VirtualPC*, and the use of behavioural monitoring tools. Packers, memory dumping and forensics all get some coverage too.

This chapter is definitely not for the faint-hearted or those that have never handled live malware before. Geeks/nerds will love it.

Chapter 10 is entitled 'Antimalware evaluation and testing' and details how anti-malware tools should be tested, and by whom (for example by *Virus Bulletin*). It also covers how *not* to test, giving examples of how poor some of the non-specialist testing can be. However, it does also offer an evaluation checklist which could be used as a handy guide for in-house product evaluation, if you really must do it yourself.

The chapter also discusses the importance of researcher ethics and sample verification, and is rounded off with a look at independent testing and certification bodies, including the likes of *Virus Bulletin*, *ICSA Labs* and *AV-Test.org*, as well as several others.

To demonstrate that there is such a thing as a perfect anti-malware solution the chapter summary includes a link to Dr Alan Solomon's 'Perfect AV' article (http://members.aol.com/drasolly/perfect.htm).

Chapter 11 completes the book with a look at 'AVIEN and AVIEWS: the future'. This chapter is really a quick summary of many of the things covered in the book as well as a look at how AVIEN and AVIEWS have adapted to the changes in the threatscape since their inception, and how they continue to adapt.

Not surprisingly the chapter ends with the suggestion that if the reader isn't already a member of AVIEN/AVIEWS they consider joining. If this suggestion were from a commercial company I would be inclined to call it shameless marketing. However, as AVIEN/AVIEWS is a non-profit organization, and I have found the benefits it provides to be very valuable, I say come and join in.

CONCLUSIONS

So, what impressions am I left with after reading the first AVIEN/AVIEWS book? My overriding impression is that this book is very well written; the whole book comes together and flows very well – which can be a difficult feat when a book has several different contributors.

The book eases the reader in gently, starting with non-technical chapters and building to some very technical ones towards the end of the book.

The pedigree and diversity of the contributors involved in this book makes it a very readable, informative, and accurate reference guide for all interested parties, be they new to the fight or old hands.

The book delivers on many of the promises it made. In fact, I would say that this is the best general malware/anti-malware book currently available, and it should be a mandatory read for anyone new to computer security in general, and anti-malware specifically.

I'm already looking forward to the second (updated) edition.