

REVIEW: "Malware: Fighting Malicious Code", Ed Skoudis

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-02/0446.html>

From: Rob Slade, doting grandpa of Ryan and Trevor (*rslade_at_sprint.ca*)

Date: 02/19/04

Date: Thu, 19 Feb 2004 16:17:17 GMT

BKMLWFMC.RVW 20031202

"Malware: Fighting Malicious Code", Ed Skoudis, 2004, 0-13-101405-6,
US\$44.99/C\$67.99

%A Ed Skoudis

%C One Lake St., Upper Saddle River, NJ 07458

%D 2004

%G 0-13-101405-6

%I Prentice Hall

%O US\$44.99/C\$67.99 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0131014056/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/0131014056/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0131014056/robsladesin03-20>

%P 647 p.

%T "Malware: Fighting Malicious Code"

Chapter one introduces, but also mixes up, all kinds of malware, attack tools, and attacks. It does eventually provide a table of types of malware, but the definitions are not very clear or explicit. Chapter two has wide ranging, but careless, information about viruses. The strictly Cohenesque definition eliminates boot sector infectors from consideration, which is rather ironic given the prominence that they are given in the chapter. There is a confused outline of infection mechanisms. Many of the assertions made are based on questionable analysis: Strange Brew is stated to be potentially dangerous because of platform independence, but there is no mention of the fact that it fails as an applet, which is the most mobile form of Java code. Random thoughts on worms are in chapter three, with defence measures seemingly a vague afterthought. Malicious mobile code is limited to active content for Web pages in chapter four. Chapter five confuses maintenance hooks and rootkits, but mostly describes remote access trojans. Trojans, or trojan horse programs, are the broadest class of malicious software, so it is not surprising that chapter six is an unfocused grab bag: what is odd is that there is so much content that is a repeat of earlier material. Chapter seven deals with "user-mode" rootkits, providing lengthy examples

which are nonetheless vague on concepts. "Kernel-mode" rootkits, in chapter eight, goes into excruciating operating system internals detail about how such software can be inserted into the system. Both chapters concentrate heavily on UNIX, with only limited mention of Windows, and both are primarily concerned about how to attack, with little attention paid to defence. ("Harden systems and apply patches.") Chapter nine theorizes about BIOS (Basic Input/Output System) and microcode malware, managing to confuse not only the two concepts with each other, but also with standard rootkits. A number of fictional attacks are outlined in chapter ten, although the "mistakes" pointed out do suggest some protective measures that might be of use. Chapter eleven lists hardware and software for building a setup to analyze malware. The book concludes with some opining in chapter twelve.

The text is much more verbose than it really needs to be, and sensational rather than precise. There is a lot of specific detail in some areas, particularly for those interested in UNIX system internals, but the material on malware itself tends to be careless, and the author is obviously much keener on attacking than defending. This work does not offer much help to those who want to fight malicious code.

copyright Robert M. Slade, 2003 BKMLWPMC.RVW 20031202

```
--
=====
rslade@vcn.bc.ca      slade@victoria.tc.ca      rslade@sun.soci.niu.edu
"If you do buy a computer, don't turn it on."    - Richards' 2nd Law
===== for back issues:
[Base URL] site http://victoria.tc.ca/techrev/
                or mirror http://sun.soci.niu.edu/~rslade/
CISSP refs:      [Base URL]mnbksccd.htm
Security Dict.: [Base URL]secgloss.htm
Security Educ.: [Base URL]comseced.htm
Book reviews:   [Base URL]mnbk.htm
                [Base URL]review.htm
Partial/recent: http://groups.yahoo.com/group/techbooks/
Security Educ.: http://groups.yahoo.com/group/comseced/
Review mailing list: send mail to techbooks-subscribe@egroups.com
                  or techbooks-subscribe@topica.com
```