Analysis of *Hacking Exposed: Malware & Rootkits*

Chris Williams

2010-11-29

Hacking Exposed: Malware & Rootkits is an excellent resource that contains medium-level[1] details on a wide range of malware and rootkit-related topics. It is very useful for understanding the concepts in question, but is relatively light on the code and gritty details.

The first few chapters cover a hypothetical scenario that demonstrates how malware is used, what the motivation is, how attackers use malware economically, *etc.* Most people who study computer forensics will already have an understanding of this material, but it is still worth reading at some point for a broader perspective and for developing an attacker's mindset.

In Part II, rootkits are covered in somewhat more detail. This disparity is odd, given that rootkits are already covered in detail by many other books, while malware is still a lesser covered topic. Unlike other texts on rootkits, however, this focuses more on an incident-response level. That is, detection and removal as opposed to implementation. In a sense, it is more defensive than the contents of *Rootkits: Subverting the Windows Kernel* and the like. In this sense, it is more useful for the IT team at a large company than for someone who performs analysis or is interested in the technical details. Chapter 5 is an interesting section on "virtual rootkits" that really isn't covered in other books. This includes rootkits that encapsulate the native operating system in a virtual machine (where it is significantly less likely to be detected) and rootkits that hijack an already-existing hypervisor. Additionally, it discusses the simpler, virtualization-aware rootkits, which change their behavior when they detect that they are running inside of a virtual machine. This increases the difficulty of detection and analysis for a reverse engineer, but is not altogether intractable.

Part III covers preventative measures, and covers antivirus techniques and solutions in some detail. There is an interesting section on the challenges of antivirus, which points out that antivirus solutions are not perfect. It is my opinion that people in general rely too heavily on antivirus products at the cost of intelligent user decisions. It goes one step further and shows that some antivirus solutions use rootkit concepts, which is potentially dangerous. I have always been an advocate of using an antivirus product as a later line of defense and eliminating the mindset of "Norton didn't detect a virus, so this file must be safe," so it is nice to see this concept in print.

So, as *Forensic Discovery* is a broad overview of computer forensics, *Hacking Exposed: Malware & Rookits* is an overview of malware and rootkits. It provides a reasonable index into malware and rootkit functionality such that it is fairly straightforward to find more in-depth information from a more focused source. In my opinion, it is written at a level that is sufficient for computer scientists, but also such that someone with average-level computer experience could follow. Thus, all computer users should at least skim this book to gain an understanding of the relatively new threats that exist on the Internet. Computer scientists should study it so that they can effectively address the threats.

[1] It is medium-level in the sense that it is not high-level but also not quite low-level.