PART I

MAC MALWARE BASICS

Before we dive into advanced malware analysis topics, it is important that you understand the fundamentals of Mac malware. In the first part of this book, we'll explore these basics, including:

- **Infection Vectors:** The means by which malware gains initial access to a system. Though most Mac malware relies on various social engineering schemes, other more sophisticated and effective methods of stealthily infecting systems are gaining popularity.
- **Methods of Persistence:** The means by which malware ensures it will be automatically re-executed by the operating system, generally on system startup or user login. Though attackers regularly abuse only a small handful of these methods, we'll cover a myriad of surreptitious means by which malware can achieve persistence.
- **Capabilities:** The malware's payload, used to achieve its goals. Cybercriminals typically create malware to pursue financial gains, whereas state-sponsored cyberespionage malware seeks to spy on users. We'll explore both.