PART II

MAC MALWARE ANALYSIS

Now that you understand Mac malware's infection vectors, persistence mechanisms, and capabilities, let's discuss how you can effectively analyze malicious samples. We'll cover both static and dynamic approaches:

- **Static Analysis:** The examination of a sample without executing it. This approach leverages various tools that can statically extract information from a sample. Often, the analysis culminates with the use of a disassembler or decompiler.
- **Dynamic Analysis:** The examination of a sample during its execution. This approach most commonly leverages passive monitoring tools, though it might employ more powerful tools, such as a debugger, as well.

Using these analysis techniques, we'll determine whether a sample is indeed malicious and, if so, answer questions such as the following: What infection vector does it use to infect a Mac? What, if any, persistence mechanism is used to maintain access? What are its ultimate objectives and capabilities?

With the answers to these questions, we can determine exactly what threat the malware poses to Mac users, as well as create detection, prevention, and disinfection mechanisms to thwart it.