PART III

ANALYZING EVILQUEST

It's time to put the universal adage "practice makes perfect" into, well, practice. In Part III of this book, you'll apply all that you've learned in Parts I and II to thoroughly analyze the intriguing Mac malware specimen known as EvilQuest. Discovered in the summer of 2020, this malware appeared at first blush to be little more than a run-of-the-mill piece of ransomware. However, further analysis uncovered something far more sophisticated.

You'll get the most out of this section by following along and performing the analysis with me. First, make sure you've created a safe analysis environment; return to this book's introduction for guidelines on doing so. Then download the EvilQuest specimen from Objective-See's Mac malware collection at *https://objective-see.com/downloads/malware/EvilQuest.zip*. Use the password `infect3d` to decrypt the malicious sample.

Ready to dive in together? Let's go!