PART III

TOOL DEVELOPMENT

You can think of the topics covered in Parts I and II as pieces of a larger puzzle. For example, Chapter 7 showed that you can leverage the *NetworkExtension* framework to detect new processes attempting to access the network, but to determine whether a process is malware or benign, you'd likely want to return to topics covered in Part I, including extracting its process arguments (Chapter 1), extracting its code signing information (Chapter 3), and checking whether the process has persisted (Chapter 5). You may even want to parse its Mach-O binary for anomalies (Chapter 2).

Now that I've covered all of these approaches in detail, it's time to pull them together. In Part III, I'll cover the design and internals of Objective-See tools that provide powerful heuristic-based malware detection capabilities. These tools are free and open source and have a track record of detecting sophisticated malware, as well as never-before-seen threats.

Part III starts by focusing on tools capable of enumerating and detecting persistent malware in real time (KnockKnock and BlockBlock). Then I'll discuss OverSight by showing how to build a tool capable of detecting

malware that surreptitiously accesses either the mic or the webcam to spy on users. Finally, I'll detail how to build a complete DNS monitor able to detect and block malware that attempts to access remote domains. While discussing the internals and constructions of these tools, I'll touch on examples of in-the-wild macOS malware they can detect.

It's important to test all security to see how it stacks up against a variety of real-world threats. As such, I'll wrap up the book by pitting our tools and detection approaches against recent threats targeting macOS systems. Which will prevail?

You'll get the most out of this part of the book if, for each chapter, you download the relevant tool's source code. This is particularly important because some chapters omit parts of the code for brevity.

All the tools referenced in this part can be found in the Objective-See GitHub repository: *https://github.com/objective-see*. If you'd like to build the tools yourself, please note that you'll need to use your own Apple Developer ID and, where applicable, your own provisioning profiles for tools that require entitlements.