The idea of malicious software as a potential threat could hardly seem novel to even the most uninformed at the dawn of our era of pervasive technology and global connectivity. The early 1970s ushered in the evolution of malicious software technologies, and their developers and users have since driven a substantial portion of the research and development agenda of the information security discipline.

Although the rules of the information security “game” seem to constantly change, the tools players use have been the same for more than 30 years: software artifacts and a handful of security practices and policies built on a few fundamental principles borrowed from mathematics, engineering, and economics. The offensive is based on a plethora of software tools that are loosely grouped under the all-encompassing term of malware, one of several neologisms that the information security community can claim as its own. Viruses, worms, Trojan horses, key loggers, dialers, stealth password sniffers, Web traffic generators, advertisement popup programs, exploits, rootkits, botnets, and zombie agents all live under the malware umbrella definition.

This special issue of IEEE Security & Privacy focuses on malware’s various forms and the threats they pose to modern networks. In putting together the issue, I sought out contributions that discuss classification, detection, containment, and removal of malicious software, as well as advances in defensive artifacts to preempt the associated threats of their offensive counterparts. The search was slightly biased toward the applied research, practical implementations, and field experiments that would give our readers insight into the tactics currently in play in the malware game.

As this issue’s guest editor, I enjoyed reading all the contributions—they proved insightful, diverse, and imaginative while maintaining a practical focus. Deciding which articles to include wasn’t a simple task, given the broad range of possible topics. The IEEE S&P staff pushed the magazine’s page length boundaries to the limit to make room for five articles, and I’m thankful that they did: the resulting combination is, I hope, well balanced and worthy of our readership’s various interests.

We start our journey with a practical study of the plausibility of malware proliferation over wireless networks. In “Studying Bluetooth Malware Propagation: The BlueBag Project,” Luca Carettoni, Claudio Merloni, and Stefano Zanero give a detailed account of a combined hardware and software artifact designed to detect and assess the Bluetooth capabilities of mobile devices in live and highly populated scenarios.

Vanessa Gratzer and David Naccache take us to the microcosm of microcontroller firmware and embedded operating systems in “Alien vs. Quine.” A clever combination of side-channel attacks and self-mutating code—technical tricks commonly associated with offensive security patterns—exemplify how malware-detection techniques can benefit from software or hardware features that are often perceived as design weaknesses.

Carsten Willems, Thorsten Holz, and Felix Freiling address malware identification and classification from a behavioral-analysis perspective in “Toward Automated Dynamic Malware Analysis Using CWsandbox.” The authors describe the implementation and use of a software tool that aims to automatically identify malicious software binaries captured “in the wild” using sandboxing technology.

A Surprise Party (on Your Computer)?
Guest Editor’s Introduction

The malware problem continues to grow as attackers fine-tune techniques to hide the true nature of the code underlying the malware. This special issue by no means constitutes a comprehensive report of all ongoing work—I encourage our readers to follow up with contributions that will help us build up a more complete playbook for the information security community and attain a better understanding about how to solve the malware problem.

Iván Arce is chief technology officer and co-founder of Core Security Technologies—an information security company based in Boston. Previously, he worked as vice president of research and development for a computer telephony integration company and as information security consultant and software developer for various government agencies and financial and telecommunications companies. Contact him at ivan.arce@coresecurity.com.