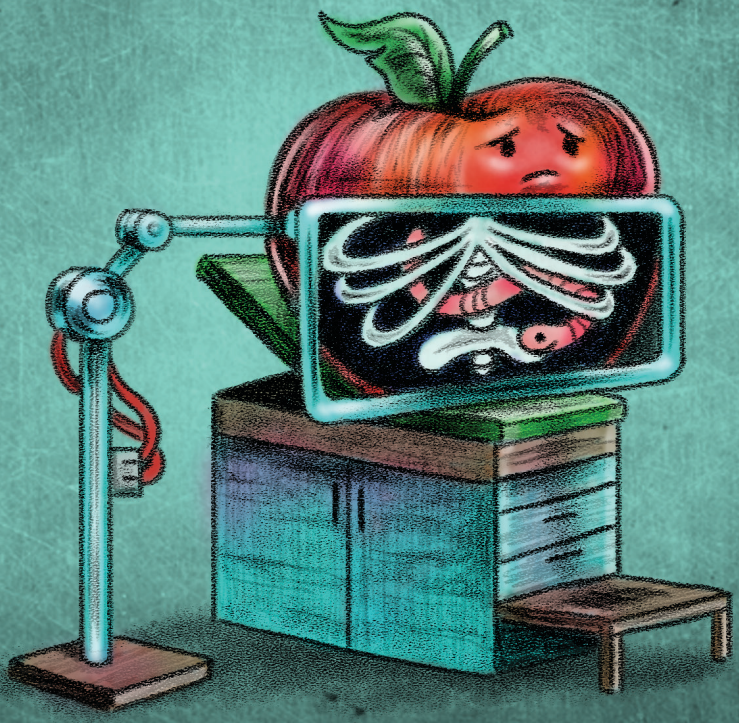
The Art of Mac Malware

The Guide to Analyzing Malicious Software



Patrick Wardle

no starch press

THE ART OF MAC MALWARE

THE ART OF MAC MALWARE

The Guide to Analyzing Malicious Software

by Patrick Wardle

no starch press

San Francisco

First printing

26 25 24 23 22 1 2 3 4 5 6 7 8 9

ISBN-13: 978-1-7185-0194-2 (print)
ISBN-13: 978-1-7185-0195-9 (ebook)

Publisher: William Pollock
Production Manager: Rachel Monaghan
Production Editors: Katrina Taylor and Hilary Mansfield
Developmental Editor: Frances Saux
Cover Illustrator: Garry Booth
Interior Design: Octopod Studios
Technical Reviewer: Tom McGuire
Copyeditor: Andy Carroll
Compositor: Jeff Lytle, Happenstance Type-O-Rama
Proofreader: James Fraleigh
Indexer: BIM Creatives, LLC

For information on distribution, bulk sales, corporate sales, or translations, please contact No Starch Press, Inc. directly at info@nostarch.com or:

No Starch Press, Inc.
245 8th Street, San Francisco, CA 94103
phone: 1.415.863.9900
www.nostarch.com

Library of Congress Cataloging-in-Publication Data

```
Names: Wardle, Patrick, author.
Title: The art of Mac malware : the guide to analyzing malicious software /
   Patrick Wardle.
Description: San Francisco : No Starch Press, [2022] | Includes
   bibliographical references and index. |
Identifiers: LCCN 2021047239 (print) | LCCN 2021047240 (ebook) | ISBN
   9781718501942 (paperback) | ISBN 9781718501959 (epub)
Subjects: LCSH: Macintosh (Computer)--Security measures. | Malware
   (Computer software)--Prevention. | Software failures.
Classification: LCC QA76.774.M33 W37 2022  (print) | LCC QA76.774.M33
   (ebook) | DDC 005.4/46--dc23/eng/20211105
LC record available at https://lccn.loc.gov/2021047239
LC ebook record available at https://lccn.loc.gov/2021047240
```

This book is dedicated to my parents,
Stephen and Norma, who patiently and
lovingly provided me both the lessons and
tools to thrive.

. . . and to Andy #UnaMas

About the Author

Patrick Wardle is the founder of Objective-See, a nonprofit that creates open source macOS security tools and trainings, and organizes the Objective by the Sea conference. Having worked at NASA and the NSA and presented at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Patrick is passionate about all things related to Mac security and spends his time finding Apple zero-days, analyzing Mac malware, and writing free open source security tools to protect Mac users around the world.

About the Technical Reviewer

Tom McGuire has been working in the security industry since the late '90s. He is the CTO of a cybersecurity firm and a lecturer at Johns Hopkins University, where he teaches reverse engineering, operating system security, cryptology, and cyber risk management. He loves his family, all things security, biotech, and the Red Sox.

BRIEF CONTENTS

CONTENTS IN DETAIL

FOREWORD

Apple's macOS—Darwin—has evolved considerably in the past two decades. From a relatively niche operating system trailing way behind Microsoft's Windows, macOS has slowly but surely gained acceptance. People all over the world started realizing its powerful capabilities, coupled with the Mac's superior hardware and integration into the Apple ecosystem, spearheaded by the iPhone.

But with widespread adoption came widespread threats. Gone were the days of the "Mac versus PC" ads, showing the PC as a sniffling, virus-infected system, while the Mac chuckles them away. Viruses, spyware, ransomware, and other malware have dramatically exploded, and by now it seems that every week some new variant emerges. Malware authors found the Mac to be a ripe breeding ground for exploitation and proliferation.

In the face of this new normal, action was needed. Although Apple integrated its own frameworks (XProtect and, more recently, Endpoint Security) and YARA antivirus signatures, there was still a gaping void when it came to intrusion detection and Mac malware detection and prevention tools.

Into this chasm stepped Patrick. "That macOS Malware guy" started churning out a cornucopia of free and effective security and analytics tools, through the Objective-See website. By now, Pat's GitHub repository sports some two dozen tools, which have managed to level the playing field a little, giving power users the ability to monitor what goes on inside their Mac, detecting (and hopefully preventing) compromises.

The tools are open source, yet it's doubtful how many people pore over sources. This is where this book fills another lacuna—explicating the ins and outs of Malware in a much-needed book. From the basics through infection vectors to the various analysis methods and techniques, Patrick elucidates Mac malware, drawing on the (unfortunately) many real-life examples.

In a perfect world, viruses—both biological and computerized—would be easy to vanquish. Not so in ours. Thus, research into how they work, and how to prevent them—whether proactively and reactively, or a combination of techniques—is paramount.

—Jonathan Levin,
Author of the "macOS/iOS (*OS) Internals" trilogy

ACKNOWLEDGMENTS

A computer is made up of countless components, crafted by many discrete craftsmen. I'm pretty sure I'm not a computer, yet I too feel composed of unique individuals and communities. Even though there is a single name on the cover of this book, you would not be holding it in your hands today without them.

First and foremost, I want to acknowledge my parents, who expertly navigated the complexities of raising a child, deftly sublimating my rebellious tendencies into a creative and independent love of learning that has benefited me ever since.

Similarly, I am forever grateful to my older brother Keelian, who always equally challenged and inspired me. Nothing like a never-ending sibling rivalry to bring out the best in us . . . right?

I also want to thank my many coworkers and colleagues at the NSA and in the larger the infosec community, whose guidance and support have been invaluable over the years. Though there are far too many to name in this short section, a few, namely my close friends and colleagues Kasey, Tom, Josh, and Jon, have had a profoundly positive influence on both my personal life and career. Others, such as the brilliant Jonathan Levin and Arnaud Abbati, have always selflessly provided indispensable technical insights and mentorship, giving me both the confidence and expertise to write this book. I am lucky to count both as close friends.

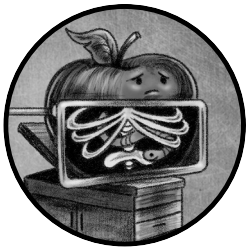
And, too, I want to personally acknowledge the many patrons of Objective-See, whose continued support made this book and my vision of free, open source Mac security tools a reality.

The companies who participate in the Friends of Objective-See programs have also helped this book see the light of day. For that, I am forever grateful. These Friends of Objective-See include, first and foremost:

Other supporting companies and products include: SmugMug, Guardian Firewall, iVerify, Halo Privacy, and uberAgent.

Last, but certainly not the least, are the many individuals who worked directly on the book. These delightful (and, yes, sometimes strict) humans kept me roughly on schedule to bring this book to fruition. First, a big mahalo to Runa Sandvik for her invaluable input and editing skills on the initial draft of this book. Also, my good friend Tom McGuire (Tmac), who put countless hours into the rather thankless job of technical editor. Finally, a big thank you to the incredibly professional and hardworking crew at No Starch Press, including founder Bill Pollock and the book's main editor, Frances Saux.

INTRODUCTION



Do Macs even get malware? If we're to believe an Apple marketing claim once posted on Apple.com, apparently, no:

> [Mac] doesn't get PC viruses. A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe without any work on your part.[1]

Of course, this statement was rather deceptive and to Apple's credit has long been removed from their website. Sure, there may be a kernel of truth in it; due to inherent cross-platform incompatibilities (not Apple's "defenses"), a native Windows virus cannot typically execute on macOS. But cross-platform malware has long targeted both Windows and macOS. For example, in 2019 Windows adware was found packaged with a cross-platform framework that allowed it to run on macOS.[2]

Regardless of any marketing claims, Apple and malware have a long history of coexisting. In fact, Elk Cloner, the first "wild virus for a home

computer," infected Apple operating systems.[3] Since then, malware targeting Apple computers has continued to flourish. Today it's no surprise that Mac malware is an ever-growing threat to both end users and enterprises.

There are many reasons for this trend, but one simple reason is that as Apple's share of the global computer market grows, Macs become an ever more compelling target to opportunistic hackers and malware authors. According to Gartner, Apple shipped over 6 million Macs in the second quarter of 2021 alone.[4] In other words, more Macs means more targets for more Mac malware.

Moreover, although we often think of Macs as primarily consumer-focused machines, their presence in the enterprise is rapidly increasing. A report from early 2020 that studied this trend notes that Apple's systems are now in use "across the Fortune top 500."[5] Such an increase unfortunately also begets an increase in sophisticated malware designed specifically to target the macOS enterprise, for purposes such as industrial espionage.

And although Apple's market share still largely lags Microsoft's, some research indicates that malicious threats target Macs equally, if not more. For example, Malwarebytes noted the following in their "2020 State of Malware Report":

> And for the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint.[6]

An interesting trend, and one that aligns with the ever-growing popularity of macOS, is attackers porting their Windows malware to macOS so that it will run natively on Apple's desktop platform. In fact, in 2020 over half of the newly discovered, unique macOS malware "species" originated on Windows or a non-macOS platform.[7] Recent examples of malware specimens that now have macOS variants include Mami, Dacls, FinSpy, IPStorm, and GravityRAT.

And why wouldn't malware authors port their Windows or Linux malware to macOS? Such malware is already feature-complete and tested in the wild on the other operating systems. By taking this malware and either porting it to (or simply recompiling it for) macOS, attackers immediately gain compatibility with a whole new set of targets.

On the flip side, attackers also appear to be investing in macOS-specific malware. For example, a report from 2020 highlights the growing number of Mac-specific malware attacks created by highly knowledgeable macOS hackers:

> All of the samples reviewed above have appeared in the last eight to ten weeks and are evidence that threat actors . . . are themselves keeping up-to-date with the Apple platform. These are not actors merely porting Windows malware to macOS, but rather Mac-specific developers deeply invested in writing custom malware for Apple's platform.[8]

As illustrated in the following examples, these developments have led to an increase in the sophistication of attacks and malware used against macOS and its users.

Use of zero-days

In a write-up titled "Burned by Fire(fox): a Firefox 0day Drops a macOS Backdoor," I wrote about how attackers leveraged a Firefox zero-day to persistently deploy a persistent macOS implant.[9]

In another report that analyzed a different piece of macOS malware, TrendMicro researchers noted,

> We have discovered an unusual infection . . . Most notable in our investigation is the discovery of two zero-day exploits: one is used to steal cookies via a flaw in the behavior of Data Vaults, another is used to abuse the development version of Safari.[10]

Sophisticated targeting

In a recent attack by the WindShift APT group, researchers noted that "WINDSHIFT was observed launching sophisticated and unpredictable spear-phishing attacks against specific individuals and rarely targeting corporate environments."[11]

In another case, researchers at Google uncovered an attack specifically "targeting visitors to Hong Kong websites for a media outlet and a prominent pro-democracy labor and political group."[12] Attributed to nation-state attackers, the attack (which also leveraged a zero-day exploit) sought to surreptitiously infect macOS users whose political views diverged from those in power.

Advanced stealth techniques

In a report on a recent Lazarus APT Group macOS implant, I noted that the group's capabilities continue to evolve, as evidenced in "a new sample with the ability to remotely download and execute payloads directly from memory," thus thwarting various file-based security tools."[13]

In "FinFisher Filleted," yet another write-up on a piece of sophisticated macOS malware, I discussed the use of a kernel-level rootkit component. I noted that the rootkit "contains the logic to remove the target process of interest, by unlinking it from the (process) list. Once removed, the process is now hidden."[14]

Bypassing recent macOS security features

In a detailed report, "All Your Macs Are Belong To Us," on a vulnerability now patched as CVE-2021-30657, I wrote about how malware was exploiting this flaw to run unsigned and unnotarized code, "bypassing all File Quarantine, Gatekeeper, and Notarization requirements."[15]

Recently I analyzed another piece of macOS malware that had been inadvertently notarized by Apple. As discussed in my analysis, once notarized, "these malicious payloads are allowed to run . . . even on macOS Big Sur."[16]

The cause of this increased attack sophistication is up for debate: Does it come in response to Mac users becoming more threat-savvy (read: less naive)?

Or is it due to the increased availability of advanced macOS security tools, an improvement to the core security of macOS, or a combination thereof?

Let's conclude this section with a well-articulated statement from a Kaspersky "Threats to macOS users" report, which sums up the Macs versus malware debate:

> Our statistics concerning threats for macOS provide fairly convincing evidence that the stories about this operating system's complete safety are nothing more than that. However, the biggest argument against the idea that macOS (and iOS as well) is invulnerable to attack is the fact that there already have been attacks against individual users of these operating systems and groups of such users. Over the past few years, we have seen at least eight campaigns whose organizers acted on the presumption that the users of MacBook, iPhone, and other devices do not expect to encounter malware created specifically for Apple platforms.[17]

All in all, it's clear that Mac malware is here to stay—in increasingly sophisticated and insidious ways.

Who Should Read This Book?

You! If you're holding this book in your hands, by all means keep reading. While a basic understanding of cybersecurity fundamentals, or even malware basics, may help you get the most out of this book, they are not prerequisites. That said, this book was written with particular groups in mind, including, but not limited to:

- **Students:** As an undergraduate studying computer science, I possessed a keen interest in computer viruses and yearned for a book such as this one. If you are working toward a technical degree and are interested in learning more about malware, perhaps to enhance or complement your studies, this book is for you.
- **Windows malware analysts:** My career as a malware analyst began at the NSA, where I studied Windows-based malware and exploits that targeted US military systems. When I left the agency, I began studying macOS threats but encountered a lack of resources on the topic. In some sense, this book aims to fill this gap. So if you're a Windows malware analyst seeking to understand how to analyze threats targeting macOS systems, this book is for you.
- **Mac system administrators:** Largely gone are the days of the homogenous Windows-based enterprise. Today, Macs in the enterprise are ever more commonplace. This has given rise to dedicated Mac system administrators and (unfortunately) malware authors focused on enterprise systems running macOS. If you are a Mac system administrator, it is imperative that you understand the threats targeting the systems you seek to defend. This book aims to provide such an understanding (and much more).

What You'll Find in This Book

Comprehensively analyzing Mac malware requires an understanding of many topics and the mastery of many skills. To cover these in a hands-on manner, this book is divided into three parts.

In Part 1, Mac Malware Basics, we'll cover foundational topics, including Mac malware's infection vectors, methods of persistence, and capabilities.

In Part 2, Mac Malware Analysis, we'll transition into more advanced topics, such as static and dynamic analysis tools and techniques. The former involves examining a sample without executing it using various tools. Static analysis often finishes with a disassembler or decompiler. Dynamic analysis is the analysis of a malicious sample while it is executing, using passive monitoring tools as well as a debugger.

In Part 3, Analyzing EvilQuest, you'll apply all that the book has taught you by walking through a thorough analysis of a complex Mac malware specimen, EvilQuest. This hands-on section illustrates how you, too, can analyze even sophisticated malware specimens.

Armed with this knowledge, you'll be well on your way to becoming a proficient Mac malware analyst.

A Note on Mac Malware Terminology

Oxford Languages defines malware as follows:

> Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.[18]

You can think of malware simply as any software written with malicious intent.

As with anything in life, there are always shades of gray. For example, consider adware that has been packaged with shareware and installed only after a user clicks "allow" without reading a long agreement. Is this considered malware? The adware authors would argue no; they might go as far as claiming their software provides a service to the user, such as ads of interest. This argument might seem absurd, but even the antivirus industry refers to such software as "potentially unwanted software" in an attempt to avoid legal challenges.

In the context of this book, such classifications are largely irrelevant, as my goal is to provide you with the tools and techniques to analyze any program, binary, or application, regardless of its malicious nature.

A Note on Safely Analyzing Malware

This book demonstrates the use of many hands-on techniques for analyzing Mac malware. In Part 3 of the book, you can even follow along in an analysis of a malware specimen called EvilQuest. But because malware is malicious, it should be handled with the utmost of care.

As malware analysts, we'll often want to purposely run the malware during the course of our research. By executing the malware under the watchful eye of various dynamic analysis and monitoring tools, we will be able to gain an understanding of how a malicious sample can infect a system and persistently install itself, and what payloads it then deploys. But, of course, this analysis must be done in a tightly controlled and isolated environment.

One approach is to use a standalone computer as a dedicated analysis machine. This machine should be set up in the most minimal of ways, with services such as file sharing disabled. In terms of networking, the majority of malware will require internet access to fully function (for example, to connect to a command and control server for tasking). Thus, this analysis machine should be connected to the network in some manner. At a minimum, it is recommended that network traffic be routed through a VPN to mask your location.

However, there are downsides to leveraging a standalone computer for your analysis, including cost and complexity. The latter becomes especially apparent if you want to revert the analysis system to a clean baseline state (for example, to re-run a sample, or when analyzing a new specimen). Though you could just reinstall the OS, or if using Apple File System (APFS), revert to a baseline snapshot, these are both rather time-consuming endeavors.

To address these drawbacks, you can instead leverage a virtual machine for your analysis system. Various companies, such as VMWare and Parallels, offer virtualized options for macOS systems. The idea is simple: virtualize a new instance of the operating system that can be isolated from your underlying environment and, most notably, reverted to its original state at the click of a button. To install a new virtual machine, follow the instructions provided by each vendor. This typically involves downloading an operating system installer or updater, dragging and dropping it into the virtualization program, and then clicking through the remaining setup.

Before performing any analysis, make sure you disable any sharing between the virtual machine and the base system. It would be rather unfortunate to run a ransomware sample, only to find that it had been able to encrypt files on your host system via shared folders! Virtual machines also offer options for networking, such as host-only and bridged. The former will allow only network connections with the host, which may be useful in various analysis situations, such as when you're setting up a local command and control server.

As noted, the ability to revert a virtual machine to its original state can greatly speed up malware analysis by allowing you to revert to different stages in the process. First, you should always take a snapshot before you begin your analysis so that when the analysis is complete, you can bring the virtual machine back to a known clean slate. During your analysis session, you should also make judicious use of snapshots, such as just prior to allowing the malware to execute some core logic. If the malware fails to perform the expected action (perhaps because it detected one of your analysis tools and prematurely exited), or if your analysis tools failed to gather the data you required for your analysis, no problem. Simply revert to the snapshot,

make any necessary changes to your analysis environment or tools, and then allow the malware to re-execute.

The main drawback to the virtual machine analysis approach is that malware may contain anti-VM logic. Such logic attempts to detect if the malware is running within a virtual machine. If the malware is able to successfully detect that it is being virtualized, it will often exit in an attempt to thwart continued analysis. See Chapter 9 for approaches to identifying and overcoming this logic and continuing your VM-based analysis unabated.

For more information about setting up an analysis environment, including the specific steps for setting up an isolated virtual machine, see "How to Reverse Malware on macOS Without Getting Infected."[19]

Additional Resources

For further reading, I recommend the following resources.

Books

The following list contains some of my favorite books on topics such as reverse engineering, macOS internals, and general malware analysis:

- "macOS/iOS (*OS) Internals" trilogy, by Jonathan Levin (Technologeeks Press, 2017)
- *The Art of Computer Virus Research and Defense* by Peter Szor (Addison-Wesley Professional, 2005)
- *Reversing: Secrets of Reverse Engineering* by Eldad Eilam (Wiley, 2005)
- *OS X Incident Response: Scripting and Analysis* by Jaron Bradley (Syngress, 2016)

Websites

There used to be a dearth of information about Mac malware analysis online. Today, the situation has greatly improved. Several websites collect information on this topic, and blogs such as my very own Objective-See are dedicated to Mac security topics. The following is a non-exhaustive list of some of my favorites:

- *https://papers.put.as/*: A fairly exhaustive archive of papers and presentations on macOS security topics and malware analysis.
- *https://themittenmac.com/*: The website of the noted macOS security researcher and author, Jaron Bradley, that includes incident response tools and threat hunting knowledge for macOS.
- *https://objective-see.com/blog.html*: My blog, which for the last half decade has published my research and that of fellow security researchers on the topics of macOS malware, exploits, and more.

Downloading This Book's Malware Specimens

If you want to delve deeper into the book's material or follow along in a hands-on manner (which I highly recommend), the malware specimens referenced in this book are available for download from Objective-See's online malware collection.[20] The password for the specimens in the collection is `infect3d`.

It's worth reiterating that this collection contains live malware. Please don't infect yourself! Or if you do, at least don't blame me.

Endnotes

1 Graham Cluley, "Macs and Malware—See how Apple has changed its marketing message," *Naked Security*, June 14, 2012, *https://nakedsecurity.sophos.com/2012/06/14/mac-malware-apple-marketing-message/*.

2 Emil Protalinski, "Cross-platform malware exploits Java to attack PCs and Macs," *ZDNet*, May 1, 2012, *https://www.zdnet.com/article/cross-platform-malware-exploits-java-to-attack-pcs-and-macs/*; Don Ovid Ladores and Luis Magisa, "Windows App Runs on Mac, Downloads Info Stealer, Adware," *Trend Micro*, February 11, 2019, *https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/*.

3 "Elk Cloner," *The Virus Encyclopedia*, *http://virus.wikidot.com/elk-cloner/*.

4 William Gallagher, "Gartner: Apple sold 1 million more Macs year over year in Q2," *AppleInsider*, July 13, 2021, *https://appleinsider.com/articles/21/07/13/gartner-apple-sold-1-million-more-macs-year-on-year-in-q2/*.

5 Jonny Evans, "Mac adoption at SAP doubles as Apple enterprise reach grows," *Apple Must*, February 3, 2020, *https://www.applemust.com/mac-adoption-at-sap-double-as-apple-enterprise-reach-grows/*.

6 "2020 State of Malware Report," *Malwarebytes Labs*, February 2020, *https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report-1.pdf*.

7 Patrick Wardle, "The Mac Malware of 2020," *Objective-See*, January 1, 2021, *https://objective-see.com/blog/blog_0x5F.html*.

8 Phil Stokes, "Four Distinct Families of Lazarus Malware Target Apple's macOS Platform," *SentinelOne blog*, July 27, 2020, *https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/*.

9 Patrick Wardle, "Burned by Fire(fox)," *Objective-See*, June 20, 2019, *https://objective-see.com/blog/blog_0x43.html*.

10 "XCSSET Mac Malware: Infects Xcode Projects, Uses 0Days," *Trend Micro*, August 13, 2020, *https://www.trendmicro.com/en_us/research/20/h/xcsset-mac-malware--infects-xcode-projects--uses-0-days.html*.

11 Taha K., "In the Trails of WindShift APT," *https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf*.

12 Erye Hernandez, "Analyzing a watering hole campaign using macOS exploits," *Threat Analysis Group* blog, Google, November 11, 2021, *https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/*.

13 Patrick Wardle, "Lazarus Group Goes 'Fileless'," *Objective-See,* December 3, 2019, *https://objective-see.com/blog/blog_0x51.html*.

14 Patrick Wardle, "FinFisher Filleted: a triage of the FinSpy (macOS) malware," *Objective-See*, September 26, 2020, *https://objective-see.com/blog/blog_0x4F.html*.

15 Patrick Wardle, "All Your Macs Are Belong To Us," *Objective-See*, April 26, 2021, *https://objective-see.com/blog/blog_0x64.html*.

16 Patrick Wardle, "Apple Approved Malware: Malicious Code . . . Now Notarized!?" *Objective-See*, August 30, 2020, *https://objective-see.com/blog/blog_0x4E.html*.

17 "Threats to macOS users," *SecureList*, September 11 , 2019, *https://securelist.com/threats-to-macos-users/93116/#malicious-and-unwanted-programs-for-macos/*.

18 Definition from Oxford Languages, *https://languages.oup.com/google-dictionary-en/*, accessed by entering `define: malware` in Google.

19 "How to Reverse Malware on macOS Without Getting Infected," *SentinelOne*, *https://assets.sentinelone.com/macos-reverse/*.

20 *Objective-See*'s Mac Malware collection, *https://objective-see.com/malware.html*.