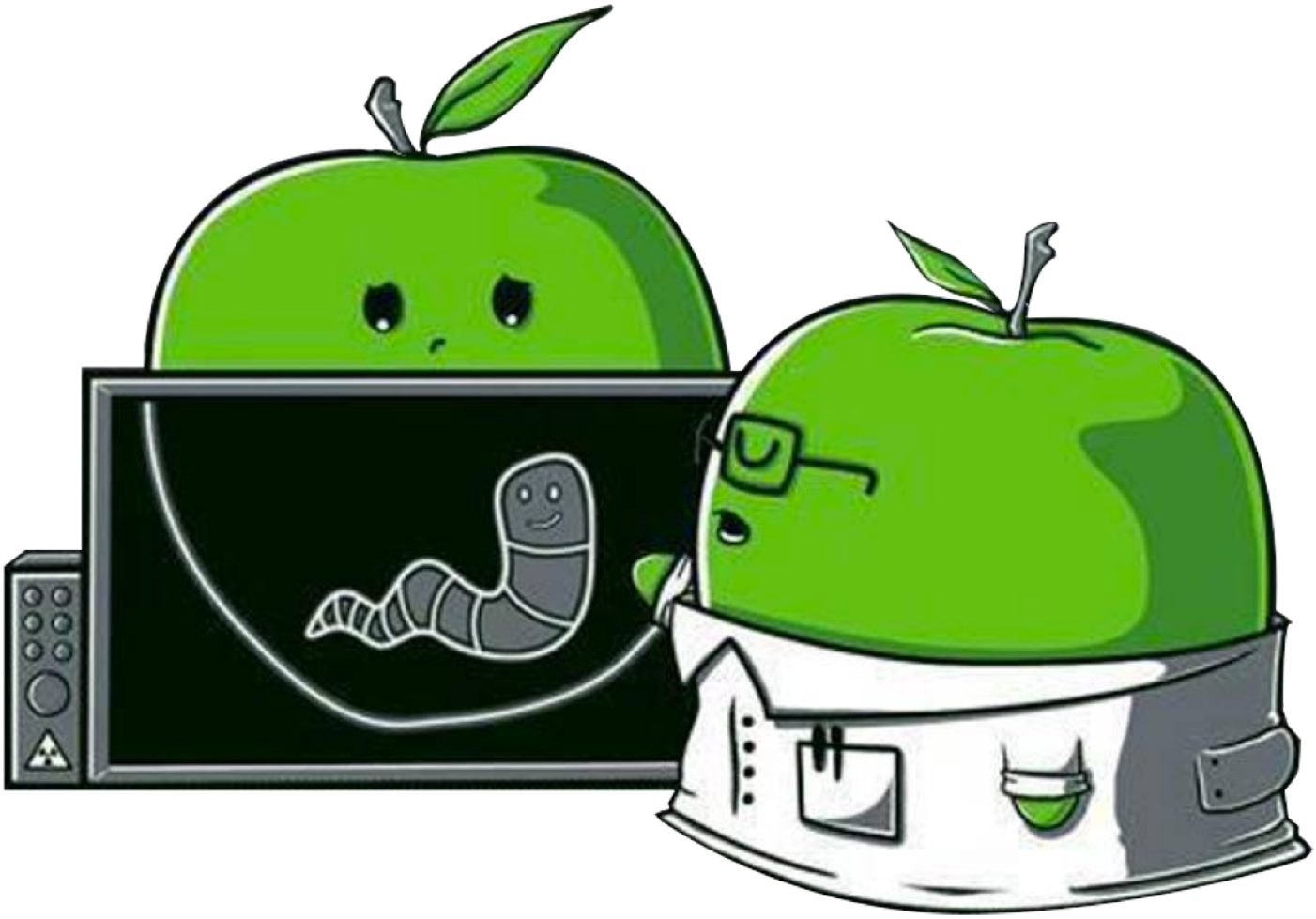


(The Art of Mac Malware) Volume 1: Analysis

Part 0x0: Introduction

📝 Note:

This book is a work in progress.

You are encouraged to directly comment on these pages ...suggesting edits, corrections, and/or additional content!

To comment, simply highlight any content, then click the icon which appears (to the right on the document's border).

Content made possible by our Friends of Objective-See:


Airo


SmugMug


Guardian Firewall


SecureMac

iVerify

Halo Privacy

Comprehensively analyzing (Mac) malware is a multi-faceted topic that requires a myriad of knowledge and skills.

In this book, we cover such knowledge and skills in a practical hands-on manner. Moreover, where relevant, links to more detailed resources are provided for the interested reader.

Starting with Mac malware fundamentals [Part 0x1], we'll then transition into more advanced topics such as static and dynamic analysis tools and techniques [Part 0x2]. To end, we'll apply all the book has taught, walking through a comprehensive analysis of a complex Mac malware specimen [Part 0x3].

Armed with this knowledge, you'll be well along the road to becoming a proficient Mac malware analyst!

> 📝 Note:
>
> If at any point you feel a little over your head, hop over to the Resources section (in Appendix B).
>
> It's full of (other) resources that cover a wide range of topics such as reverse engineering, macOS internals, and general malware analysis.

Acknowledgements

First and foremost, I want to thank my many friends and colleagues in the info-sec community whose guidance and support have been invaluable over the years!

I want to personally acknowledge and thank the many patrons of Objective-See, whose continued support made this book a reality.

I also want to thank the companies and products who participate in the "Friends of Objective-See" program:

Airo AV (https://www.airoav.com/):
Providing antivirus protection exclusively for Mac OS.


SmugMug


Guardian Firewall


SecureMac


iVerify

Halo Privacy

...as they too have helped this book see the light of day!

Finally, a big mahalo to Runa Sandvik for her invaluable input and editing skills!

📝 Note:

Want to support us?

- If you're an individual, join us on patreon!
- If you're a company, join our "Friends of Objective-See" program!

Mahalo 😇

Macs vs. Malware

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

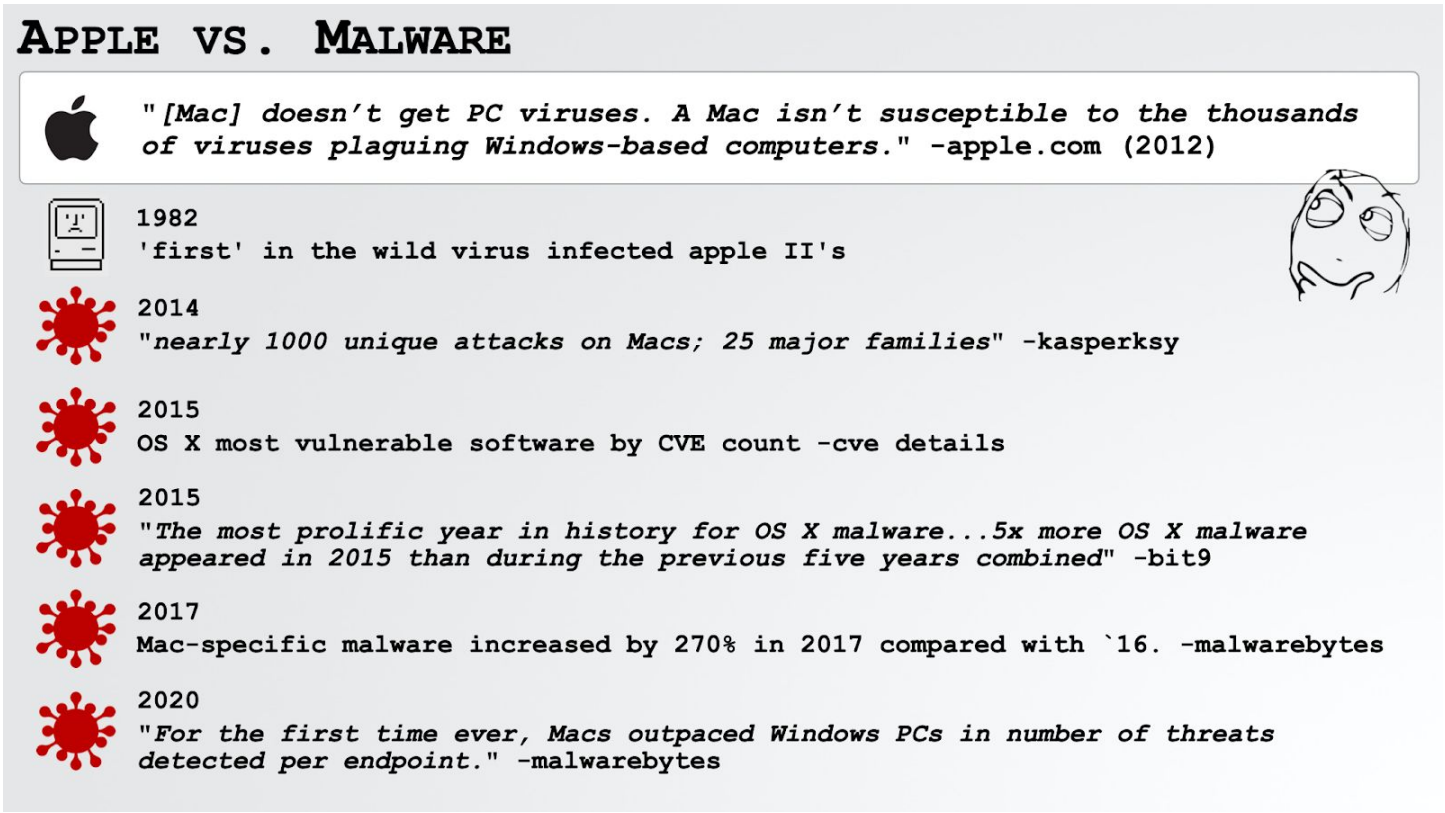
> *"[Mac] doesn't get PC viruses. A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe without any work on your part"* [1]

Of course this statement was both deceptive and inaccurate, and (to Apple's credit) has long been removed from their website [1].

> 📝 Note:
>
> The "truth" of this nuanced statement lies in the fact that due to inherent cross-platform incompatibilities (not Apple's "defenses"): a native Windows virus cannot directly execute on macOS.
>
> However even this claim is rather subjective as was highlighted in 2019 by a Windows adware specimen targeting macOS users. The adware was packaged with a cross-platform framework (Mono) that allowed Windows binaries (.exes) to "natively" run on macOS!
>
> See:
> "Windows App Runs on Mac, Downloads Info Stealer and Adware" [2]
>
> And, even back in 2012, cross-platform malware could be found targeting both Windows and macOS:
>
> *"a single piece of malware that can infect both Windows and Mac OS X computers"* [3]

Interestingly, Apple and malware have a long history together. In fact, Elk Cloner [4], the *"first wild virus for a home computer"* [4], infected Apple operating systems!

Since then, malware targeting Apple computers has continued to flourish (albeit to a lesser extent than on Windows systems):



A brief timeline of Apple vs. malware.

Today, it's no surprise that Mac malware is an ever growing threat ...to both end users and to the enterprise.

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 3.977 million macOS units in Q1 2019"* [5]).

In other words:

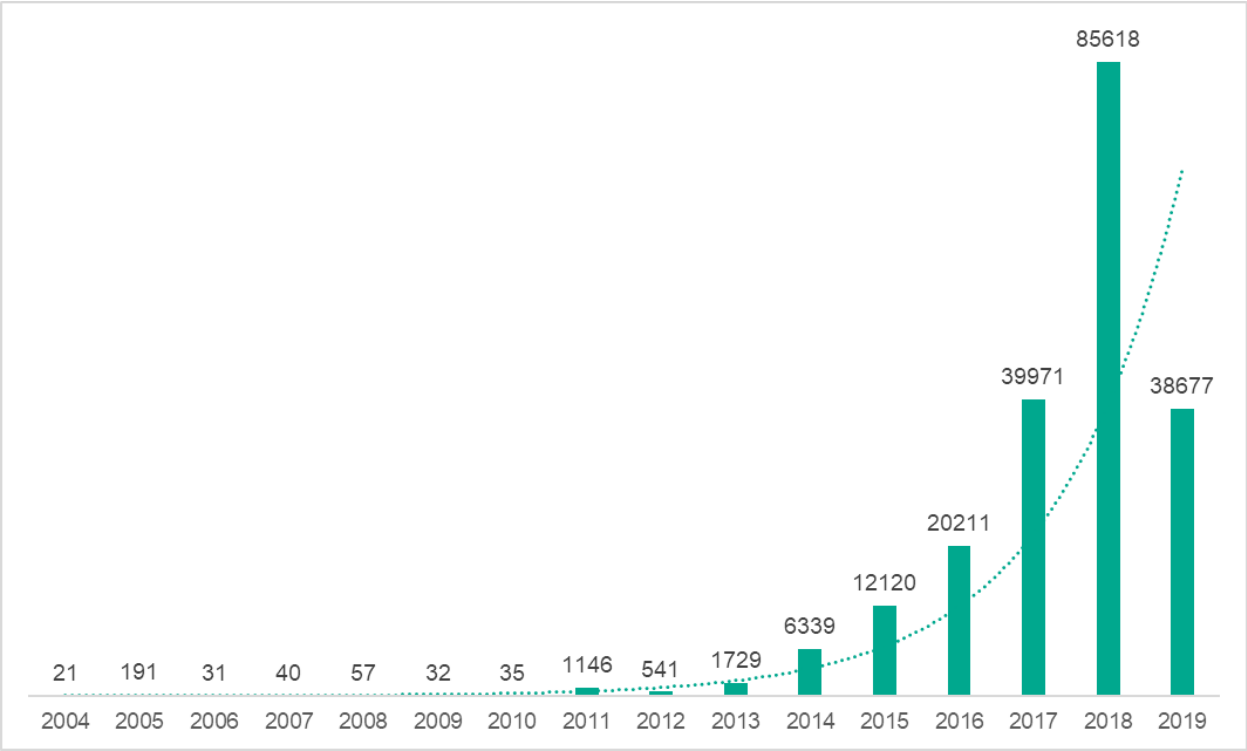
more Macs → more targets → more Mac malware

It is also important to note that although Macs are often thought of as primarily consumer-focused machines, their prevalence in the enterprise is rapidly increasing. A report from early 2020 that studied this trend, boldly states, *"the Mac is an enterprise machine"*, and notes that *"Apple continues to grow in the enterprise with its systems in use across the Fortune top 500"*. [6] Such an increase (unfortunately), also begets a parallel increase in sophisticated attacks and malware, designed specifically to target the macOS enterprise (i.e. industrial espionage).

And although Apple's market share still (largely) lags Microsoft, there is some research indicating that Macs are equally (if not moreso) targeted by malicious threats. For example, Malwarebytes noted in their "2020 State of Malware Report":

> *"And for the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint."* [7]

Kaspersky, in a 2019 report, "Threats to macOS users" [8] also noted a sharp uptick in threats (malware and adware) targeting Macs:



"The number of malicious and potentially unwanted files for macOS, 2004–2019" [8]

📝 Note:

1. Such statistics generally include adware (and/or "potentially unwanted programs").

2. The distinction between malware and adware is rather nuanced and their differences continue to blur. As such, we generally won't differentiate between the two; referring to both simply as malware.

3. Of course as Apple improves the security of macOS, it becomes more difficult for

> malware (and adware) to successfully infect Mac computers.
>
> However, this is unlikely to pose a true obstacle for motivated malware authors.

Interestingly (though unsurprising), a report [9] from 2020 also highlights the growing trend of uniquely 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."* [9]

As illustrated in the following examples, such depth and knowledge has led to an increase in the sophistication of attacks and malware against macOS and its users:

- Use of 0days:
  "Burned by Fire(fox): a Firefox 0day Drops a macOS Backdoor"

  "Via a Firefox 0day, the attackers persistently deployed a macOS binary …[a] persistent payload of a rather sophisticated targeted attack against cryptocurrency exchange(s)" [9]

- Sophisticated Targeting:
  "In the Tails of WINDSHIFT APT"

  "WINDSHIFT was observed launching sophisticated and unpredictable spear-phishing attacks against specific individuals and rarely targeting corporate environments" [10]

- Advanced (Stealth) Techniques:
  "Lazarus Group Goes 'Fileless'"

  "Lazarus group continues to target macOS users with ever evolving capabilities ...[such as] a new sample with the ability to remotely download and execute payloads directly from memory!" [11]

- Bypassing (recent) macOS Security Features:
  "New Mac malware uses 'novel' tactic to bypass macOS Catalina security"

> *"Security researchers ...have discovered a new Mac malware in the wild that tricks users into bypassing modern macOS app security protections."* [12]

Whether this increased attack sophistication is in response to Mac users becoming more threat savvy (read: less naive) and increased availability in free macOS security tools, or Apple improving the core security of macOS, or a combination thereof, is open to debate.

Kaspersky's 2019 "Threats to macOS users" report [8] sums up the "Macs vs. Malware" discussion quite articulately and concisely:

> *"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."* [8]

All in all, it's clear that Mac malware is here to stay ...and that both its sophistication and insidiousness will only continue to increase.

Up Next

With the increased prevalence and sophistication of malware targeting Apple's desktop OS we must respond! And, (as cliche as it might be), knowledge is truly power.

As such, read on! This book provides the knowledge to comprehensively understand and combat these insidious threats.

> 📝 Note:
>
> For the interested reader who wants to delve deeper or follow along in a hands-on manner, the (majority of the) malware specimens referenced in this book are available for download from Objective-See's online malware collection [12].
>
> The password for the specimens in the collection is: infect3d

> ...and it’s worth reiterating that this collection contains live malware, so, please don’t infect yourself!

References

1. “Macs and Malware – See how Apple has changed its marketing message”
https://nakedsecurity.sophos.com/2012/06/14/mac-malware-apple-marketing-message/

2. “Windows App Runs on Mac, Downloads Info Stealer and Adware”
https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/

3. “Cross-platform malware exploits Java to attack PCs and Macs”
https://www.zdnet.com/article/cross-platform-malware-exploits-java-to-attack-pcs-and-macs/

4. Elk Cloner
http://virus.wikidot.com/elk-cloner

5. “Apple’s share of global computer market grows”
https://www.cultofmac.com/618730/q1-2019-pc-market-apple-mac-gartner/

6. “Mac adoption at SAP doubles as Apple enterprise reach grows”
https://www.applemust.com/mac-adoption-at-sap-double-as-apple-enterprise-reach-grows/

7. “2020 State of Malware Report”
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report-1.pdf

8. “Threats to macOS users”
https://securelist.com/threats-to-macos-users/93116/#malicious-and-unwanted-programs-for-macos

9. “Four Distinct Families of Lazarus Malware Target Apple’s macOS Platform”
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

10. “Burned by Fire(fox) part i: a firefox 0day drops a macOS backdoor”
https://objective-see.com/blog/blog_0x43.html

11. “In the Tails of WINDSHIFT APT”
https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf

12. “Lazarus Group Goes 'Fileless': an implant with remote download & in-memory execution”
https://objective-see.com/blog/blog_0x51.html

13. “New Mac malware uses 'novel' tactic to bypass macOS Catalina security”
https://appleinsider.com/articles/20/06/18/new-mac-malware-uses-novel-tactic-to-bypass-macos-catalina-security

14. Objective-See’s Malware Collection
https://objective-see.com/malware.html