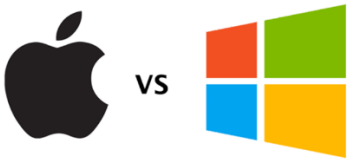
THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

June 2022

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

Apple vs Microsoft OS Security



Disclaimer: We all know the famous Operating System advertisement campaign that was launched by Apple to display, make fun of, and stereotype the differences between a Macintosh Computer user and a Windows PC user. Well… this newsletter isn't about that competition which still burns today, but rather to discuss what led so many users to believe and still believe that one operating system vendor is more secure than another. For this newsletter, while virus and malware mean different things, they will be used interchangeably to describe harmful computing threats.

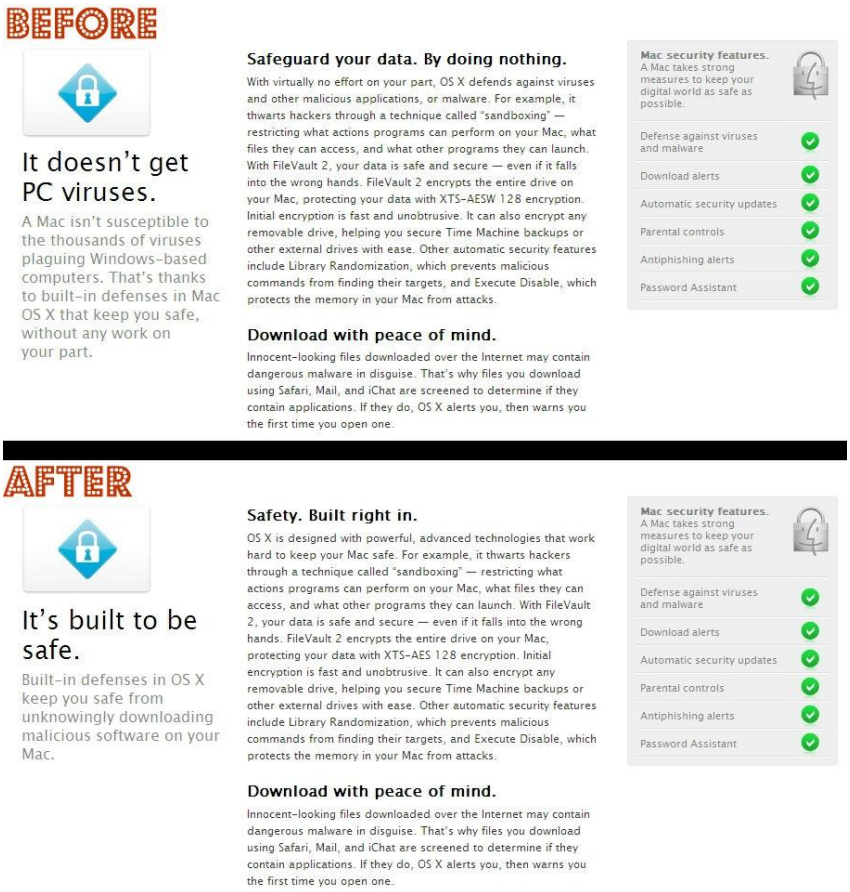
Advertisement and Compatibility of Viruses

Once upon a time, Macintosh computers (Mac) were considered more secure than their Windows Personal Computer (PC) counterparts. Many believed and still believe it was because the operating system (OS) was much more secure because of advertisements comparing their competitors' issues and training online stating as such that still exists to this day.

US version: https://www.youtube.com/watch?v=V0feR5grSa4

UK version: https://www.youtube.com/watch?v=iY1iSocnPw0

The famous line "Macs don't get PC viruses" was true at one point, but misleading due to compatibility issues between both platforms. Macs do get viruses, but they are viruses created on a Mac for Macs. Apple touted this security on their website at one point which was promptly changed after complaints were received about implying a Virus free security claim.



Outdated training video information from 2014 @58minutes discussing Mac OS security being as simple as pushing the update button:

https://www.youtube.com/watch?v=wSPisJXyjso

Macworld.com, a website dedicated to all things Mac, in 2021 stated:

> As we've explained above, **it's certainly not an essential requirement to install antivirus software on your Mac**. Apple does a pretty good job of keeping on top of vulnerabilities and exploits and the updates to the macOS that will protect your Mac will be pushed out over auto-update very quickly. Dec 1, 2021
>
> https://www.macworld.com › Software › Feature
>
> Macs can get viruses, but do Macs need antivirus software?

The article was later modified to downplay the threat due to statements made by Craig Federighi, Apple's software chief, in the Apple vs Epic Legal trial. Whether or not this was the only reason for the change has not been determined.

Do Macs get viruses? Do Macs need antivirus software? The answer isn't as simple as it may seem. In this article, we look at the dangers faced by Mac users and the pros and cons of using Mac antivirus software.

The Mac has historically been considered to be safe and secure for a number of reasons that we will go into below, but in recent years that has shifted considerably. In its report on the State of Malware in 2019 here, Malwarebytes said it saw a: "Significant rise in the overall prevalence of Mac threats, with an increase of over 400 percent from 2018".

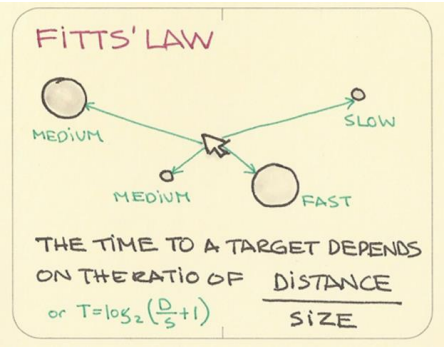
The good news is that in 2020 the amount of malware detected on macOS actually decreased by 38 percent, according to the same security company. But before you breathe a sign of relief, Malwarebytes states that the worst kind of malware, namely "backdoors, data stealers, and cryptocurrency stealers/miners, increased by more than 61 percent" in 2020.

But it's not only Malwarebytes that is reporting that viruses on the Mac is something to be concerned about: Apple is too! In May 2021 Apple's software chief Craig Federighi took the stand at the Apple vs Epic trial and said that: "Today, we have a level of malware on the Mac that we don't find acceptable."

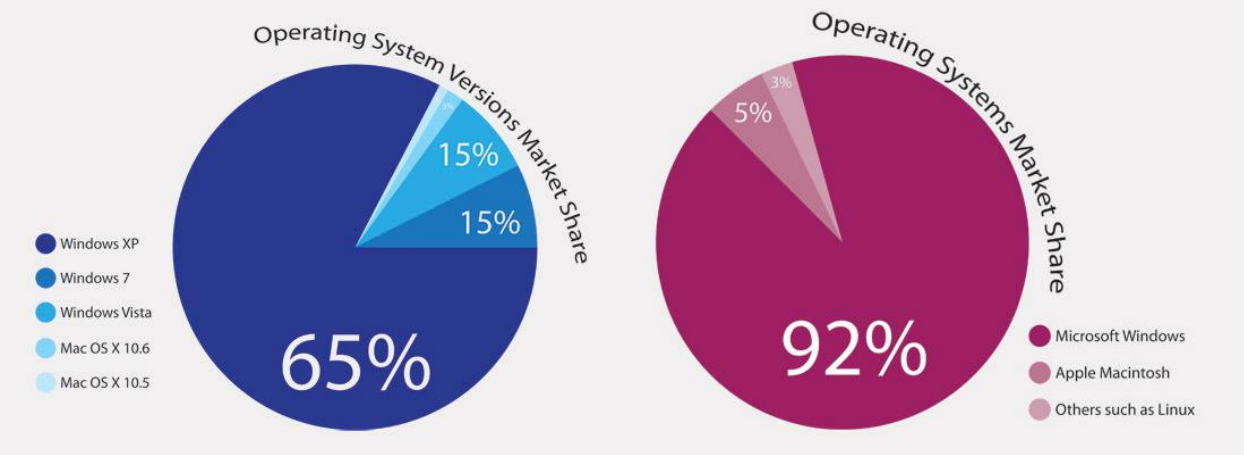
Macs do get viruses and it can be said that the number of viruses that exist is in proportion to the usage of Macs, just as the number of viruses is proportional to the number of PCs in use. It should be noted that the first computer virus called Elk Cloner, written by a 15-year-old as a joke, could infect the boot sectors of Apple II computers and spread via floppy disk. This predated the existence of the PC and started the propagation of malware trends. So contrary to what we see online and the advertisements we see everywhere the Mac is no stranger to viruses.

What audience is the best target to compromise?

The largest audience. For someone with malicious intent to spend time writing an exploit and get the best payout, it must affect as many systems as possible. What better way to do this than to affect the one that is most widely used?



Statistics around the web may show some discrepancies of a few percentages off but all of them clearly show the dominant use of the Windows Operating System.

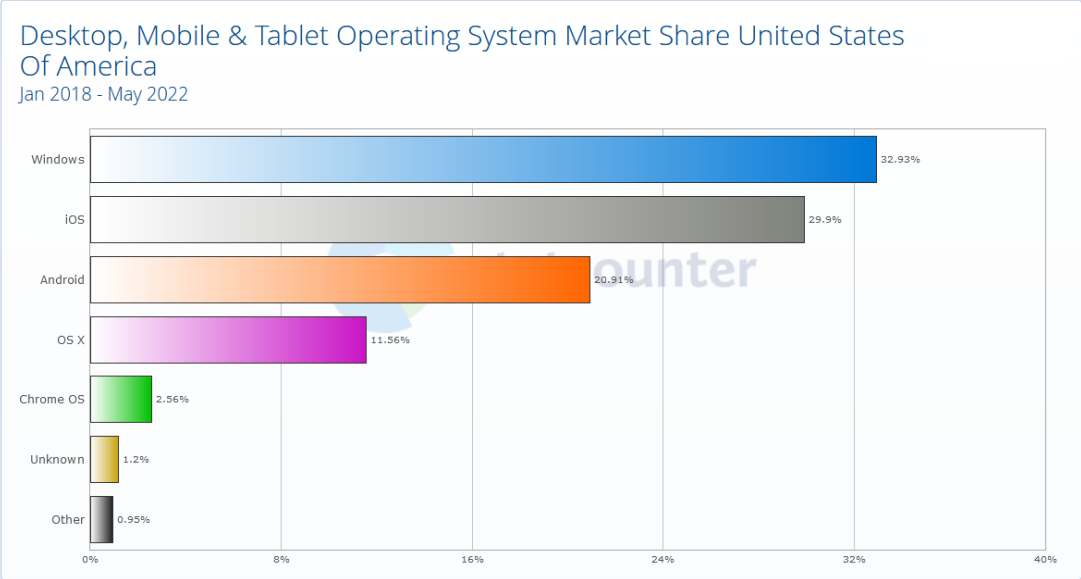


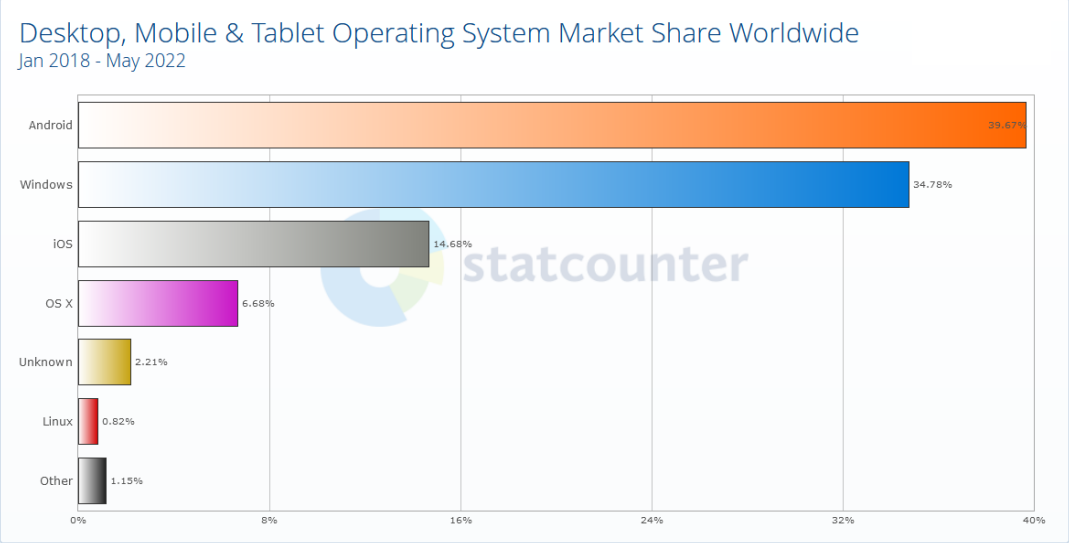
Microsoft software became so popular that items such as MacCharlie and DOS Compatibility cards were being sold for Macintosh systems so that it could use Microsoft word and other processing utilities.

Microsoft had collaborated with IBM, Dell, HP, Sony, Toshiba, Gateway and many more companies to ensure compatibility with their hardware and eventually Microsoft even started making software for the Mac which removed the need for extra hardware on the Mac to run the software. As a result of the increase in use, users were bombarded with malware, but this was more so on the PC side than the Mac side.

In the years 2018-2022

Both Microsoft and Apple have expanded to more computing platforms (phones, tablets, TVs, laptops, cars, smart home devices, etc…) that serve as interchangeable companion conduits of data. With this expansion of use Apple gained a much larger market share than it once had especially in the United States versus Worldwide. Although IOS adoption was not as worldwide, the apple market share did increase and has since garnered the same attention for malware as the PC.





In February of 2020, Malwarebytes (Antivirus company), released a report of the detections found on the Mac which outpaced the number of threats on the PC.

https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report.pdf

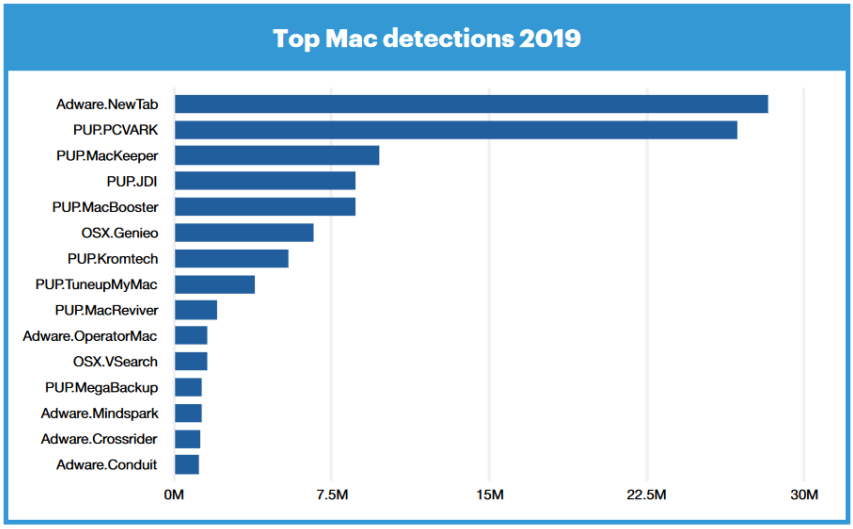


Figure 19. Top Mac detections in 2019

This report was also downplayed on many sites, but the threats are real. Even if only one machine is compromised this could lead to lateral movement within our network, allow for detection of other internal systems, internal data tampering/exfiltration, and harm to the institution and individuals.

The debate over which operating system is more secure will go on as long as there are competing operating systems. Regardless of which operating system you are using, it is important to apply security best practices based on the system you are using.

Below are the best practices for securing your device. Using built-in security features are just a start for securing your system and antivirus software can protect your device even further.

Best Practice Securing your Windows PC

Best Practice Securing your Macintosh

If at any point you believe that your PC or Mac doesn't have sufficient security, please reach out to security@bsd.uchicago.edu for assistance! We are here to help!