Crossing the Digital Divide (v55)

"Mac Attack"

By Joseph Feigon for the Observer

It's been a crazy these past few weeks – big weather, wet ground, toppled trees, Internet outages. A few days of sunshine, the ground is drier, the fallen limbs are cut, and the driveway in serious need of more 'rented' rock.

This week's column is about the Mac, viruses, malware, and truth (not the alt-fact kind), and was written by Thomas Reed , a content contributor for Malwarebytes, a software/ security vendor. Malwarebytes is the one piece of software that has literally saved my clients thousand$ in averting infected computers.

Posted March 8, 2017 by Thomas Reed

There are many Mac security myths circulating among users. So how can you tell if the advice you're reading is fact or fallacy? Read on to find out!

Fallacy: Macs don't get viruses

The idea that there are no viruses for the Mac goes back to the beginning of Mac OS X, at the very beginning of this millennium. Most people associate this idea most strongly with the "I'm a Mac/I'm a PC" commercials from a decade ago, such as this one that ran in 2006:

Unfortunately, this is a myth. As with most good myths, though, there's a slight element of truth.

Technically speaking, a virus is malware that spreads by itself, by attaching itself to other files. By this strict definition, there are no Mac viruses. However, by that token, there also aren't very many Windows viruses these days, either. Viruses have mostly disappeared from the threat landscape.

The average person, though, understands a virus to be any kind of malicious software. (A better term for this is "malware.") Since there definitely is malware for the Mac, as well as a plethora of other threat types, the spirit of the "there are no Mac viruses" claim is completely false. Don't allow yourself to be misled!

Fact: There's not much Mac malware out there

True malware is malicious in nature—thus the name, **mal**icious soft**ware**—with the goal of stealing or scamming data or money from the user. Examples of malware are backdoors that provide access to the computer, spyware that logs keystrokes and captures pictures with the webcam, ransomware that encrypts the user's files in order to hold them for ransom, and other such nefarious programs.

On the Mac, true malware is rare. A "big spike" of new Mac malware happened in 2012, when 11 new pieces of malware appeared. The average Mac user has never seen any malware.

So why should Mac users be concerned? Because other threats are a rapidly growing problem on the Mac. Over the last several years, there has been an increasing amount of adware and Potentially Unwanted Programs (PUPs) for the Mac.

Adware is software that injects ads into websites where they don't belong and changes your search engine to a different one. Adware is designed to scam advertisers and search engines. The infected Macs are no more than a vehicle for generating revenue fraudulently from advertisers and search engines, who pay these adware-producing "affiliates" for referrals.

PUPs are programs that are generally unwanted by users. These can include so-called "legitimate" keyloggers (marketed as a means for monitoring your kids or employees), scammy "cleaning" apps (Macs don't need that kind of cleaning), supposed "antivirus" or "anti-adware" apps that don't actually detect anything, and so on.

Adware and PUPs are a serious problem on the Mac right now. Although these things are not malware, they are a huge nuisance. Worse, they can create security vulnerabilities that make it more likely for you to get infected with actual malware. For example, in 2015, a vulnerability in a common PUP (MacKeeper) was used to install malware on Macs that had MacKeeper installed.

Fallacy: Macs are more secure than Windows

Many years ago, Apple abandoned the old "classic" Mac system in favor of one based on Unix, a mature and security-oriented system. Apple has made some great security improvements to macOS in recent years, and as a result, Macs are more secure today than they ever have been.

Of course, nothing is ever perfect, and macOS security is certainly far from it. There are plenty of ways to circumvent Mac security. Add to this the fact that security of Windows has improved over the years as well and it becomes difficult to say which system is more secure.

As with other such myths, there's an element of truth here, though. Macs certainly suffer under a far smaller burden of threats than Windows. Many thousands of new Windows malware variants appear every day, while it's a busy *month* in the Mac world if more than one new piece of malware appears. This means that, although there may not be

any explicit, major security differences between the two systems, Macs do tend to be statistically safer simply due to the smaller number of threats.

Fact: macOS has built-in anti-malware software

Although this feature is well-hidden from the user, and cannot be turned off, this is true. Apple's anti-malware software is called XProtect, and it consists of some basic signatures for identifying known malicious apps.

When you try to open an app for the first time, the system will check it against the XProtect signatures. If the app matches one of those signatures, the system won't allow it to open.

Of course, there are a couple problems with XProtect. First, of course, as with any signature-based detection, it can only detect and block malware that Apple has seen before.

More importantly, though, it only detects malware. Since the vast majority of the threats for Macs are adware and PUPs, that leaves a lot that it doesn't protect against. You shouldn't rely on XProtect as your sole protection against threats, but nonetheless, this is very good layer of protection to have as an integral part of the system.

Fallacy: Macs don't need security software

Antivirus software has gotten a bad rap on the Mac over the years. Thanks to historically low incidence of Mac malware, coupled with the system problems that some antivirus programs have been known to cause, Mac users are skittish about installing security software. Making matters worse, Mac "experts" will tell people that they don't need security software, because macOS contains all the protection they need.

However, the number of Mac users infected by malware and other Mac threats has had exponential growth since 2010, when adware and PUPs weren't really a thing on the Mac yet and when new malware sightings were few and far between. We're seeing large numbers of people infected with Mac threats every day, on a much larger scale than even just a few years ago.

Clearly, there is an epidemic problem with threats—mostly adware and PUPs—on the Mac, and also clearly, the built-in security in macOS is not adequate to deal with this problem. It is becoming increasingly necessary for Mac users to have an additional layer of security, and in particular, to have something that is effective against adware and PUPs, which are the biggest problem. If you're a Mac user, you might consider

downloading software such as Malwarebytes Anti-Malware for Mac, which removes adware, PUPs, and malware for free.