Helping User Groups Discuss and Understand Malware on Macs

by ugabadmin | Sep 17, 2016 | Leaders, Resources, User Group How To, User Group Meeting Materials | .et_post_meta_wrapper

By Rick Ortiz

Apple users have for the most part been protected from many of the viruses and malware issues experienced on the PC. But with the popularity of Apple products over the past decade, those wanting to take advantage and compromise your computer use experience has grown. Most recently, applications, search engine hijacks and web browser plug-ins are the culprits of what many Mac users think are “viruses.” This has become a popular discussion topic at user group meetings. So to help user groups, we are providing group leaders with a meeting guide and how you can address and discuss this issue at your meetings. Click on *read more* below to continue.

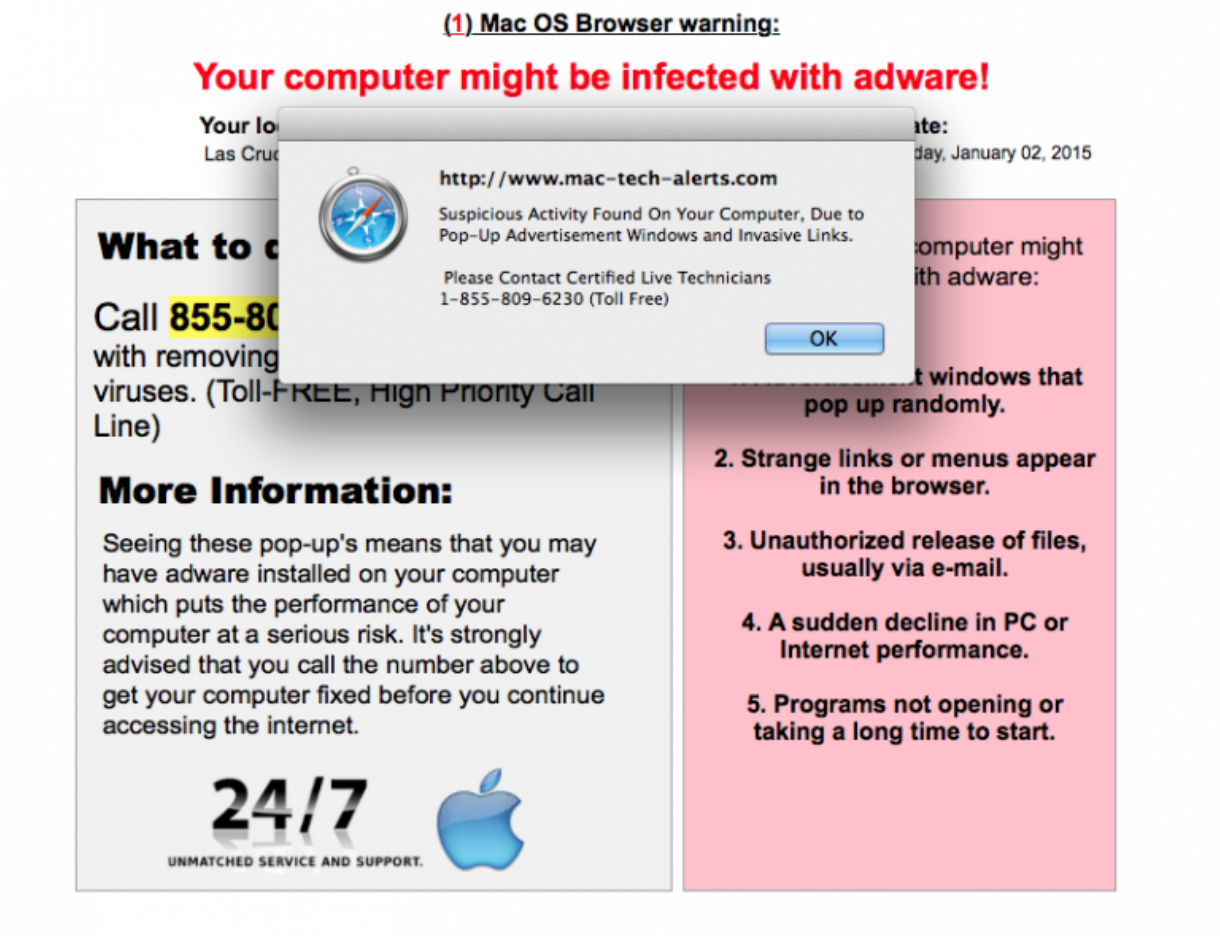
I. Overview

When discussing security, hacks, viruses and malware

with user group members, there are three major areas to discuss with them. First, there are internet issues which will try and deceive them with fake web pages and pop-ups. Second, is deceiving software they may think is legitimate that is actually bogus software which then creates an annoyance for them. The final area that tends to cause or lead to more issues, is their web browser being compromised by misleading search engines or bogus search plungins being installed. We will take a look in more detail at these areas and then discuss how to fix and offer resources that can assist in dealing with these issues.

II. Web Browser pop-up

As users are on the internet, fake ads, bogus links in emails or search engine results may redirect them to a page that pop-ups and tells them their Mac is infected with a virus. Usually there is a phone number listed which informs the user to call it immediately. Lets get right to the point. This is all a SCAM. Do not call, do not let them control your computer screen and do not give them your credit card number.



credit: thesafemac.com

How to Fix: If the user has fallen for the scam, here are some steps they can take. Immediately have them call their credit card company to dispute or cancel the charge. Unfortunately they may need to cancel that credit card number as the bank may feel it was compromised.

There may also still be some screen sharing software installed on the computer. Typically it was a one time session download software that can easily be found in the download folder and thrown away. But another place to check is in System Preferences > User and Groups > Login Items. Sometime you may find screen

sharing software listed there that starts automatically at login. You can select and hit the minus sign to remove it. A more advanced check is to hold down the option key and go under the Apple Menu and select System Information. Under System Information look in the left column for Software > Installations. You can sort by date and find if any recent software was installed. This will help you locate in your application folder any screen sharing software you may need to remove.
The biggest issue with the pop-ups is the user can't figure out how to get rid of the window or it keeps popping up after a restart. Part of the issue is because Apple introduced a feature called Auto Resume where it creates a saved state of the application. When you reopen certain applications and you did not close a file or web page in this case that was open, it re-opens to the last page you had open automatically. So to stop the issue, go to the Apple Menu and select Force Quit. Force Quit the web browser application with the fake pop-up. Here is the trick. Before attempting to open the web browser again, hold down your SHIFT key on the keyboard and while holding that down, click the web browser icon in the dock. This will force the browser to open the default page rather than the "saved state" of the malicious page.

III. Malicious Software

Along with web browser pop-ups, malicious software may be downloaded automatically and then request

an install into your computer. Again this is typically generated when you go to a web page, and a window pops up suggesting you need install some form of an update. Typically it masks itself as a Java or Flash Player update. The user believes they need to do this update and as a result malicious software gets installed. This may also be downloaded when you do a web search for software and there are bogus results that will install the malicious software. The more popular names of software to get installed are applications like MacKeeper, Zip Cloud, Mega Backups, Mac Cleaner, and a variety of other applications. Typically these applications begin to take over the menu bar, pop up windows in the Finder and create an annoyance outside of the web browser. Typically this is known as Adware as these applications inform the user that their Mac now has problems and viruses that their software can fix it. So they bait the user into believing there is a problem, then suggest the only way to fix it is to pay them for the software.

How to Fix: If the user has installed this software, there are two ways to address this. First we will repeat what was stated above regarding recently installed software. We want to find out what was installed to make sure we remove it. Hold down the option key and go under the Apple Menu and select System Information. Under System Information look in the left column for Software > Installations. You can sort by date and find if any recent software was installed. This will help you locate any unwanted software that was installed. The user may need to remove this software manually or they can use a popular piece of software used to address this issue called Malwarebytes (formerly AdwareMedic). This software is easy to install and can remove most of the malicious software that

was installed and its associated hidden components. Again, it may not catch all of it, so taking a look at installed software is a good idea to make sure it is completely removed (links provided below)

IV. Search Engine and Plugin Hijacks

Typically when one or both of the issues above has occurred, some hidden search hijacks may take over your web browsing experience. Safari, Firefox and Google Chrome are the most popular browsers for the Mac. Along with the install of malicious software, it may also alter your home page and take over your default search engine, along with installing browser extensions of plugins. So instead of going to your default home page such as google.com, apple.com, etc., you now get a new search engine page that will alter or redirect your search results. Typically if your home page has been changed, your default engine has been changed as well. So no matter how you search on the web, you get redirected to the hijacked results page. A more recent feature of web browsers are extensions or plugins. These were designed to enhance your web experience. But malicious plugins have been made that also impact your search function and creates unwanted pop-up or ads in your web browser experience.

How to Fix: Typically Malwarebytes does a good job removing malicious plugins from your browser, but may not fix your hijacked search engine results. The best way to fix this is to go to the web browser preferences

under the applications menu. Typically under the general settings it will list Homepage. That needs to be changed to the page you want loaded. Also while in preferences look for a Search section. Make sure you select the default search engine you want to use. Also make sure you remove any unrecognizable or unwanted search engines. One last place to check is for a Extensions or Plugins section. Make sure to remove items that seem suspicious or are unrecognizable.

V. Resources

This guide is intended to help user group leaders present and inform their members about protecting their Mac experience. Below are a list of resources that can help and expand on this article.

Malwarebytes- Adware and Malware removal for Mac
The Safe Mac- Mac Blog for Malwarebytes /
Suggested Tech Guides from Malwarebytes
Apple Support Articles:
https://support.apple.com/en-us/HT203987
Apple Security Updates:
https://support.apple.com/en-us/HT201222

Rick Ortiz is an Apple Certified Trainer, Technical Coordinator, and Support Professional. He currently serves on the User Group Advisory Board