MALWARE

VIRUS'S, ADWARE, SPYWARE, PUPS (POTENTIALLY UNWANTED PROGRAMS) AND THE SCAMS…

INTRODUCTION

- A few years ago I created a presentation primarily about Adware for the beginners group. I've been hearing discussions again about malware, in our email group, and other Macintosh discussion groups. So We (core group) thought it was worthy of a full main meeting topic.
- This is not always a easy topic to discuss.
  - I remember a viral video on the internet many years back of grown man sticking his fingers in his ears and yelling LA-LA-LA-LA as a traffic cop tries to give him a ticket. Maybe it worked for him at three, but I doubt the cop would withdraw the ticket as an adult. Some wish to believe there is no threat to Macs.
  - On the other hand some are panicking, running around with their hair on fire, convinced all the world's Macs will be rendered useless within a month, looking for some magic bullet program to make them 100% risk free. Doesn't exist.
  - Adware started becoming an issue for the Mac OS several years ago. Has it increased over the years yes. An epidemic NO.

MALWARE DEFINITION

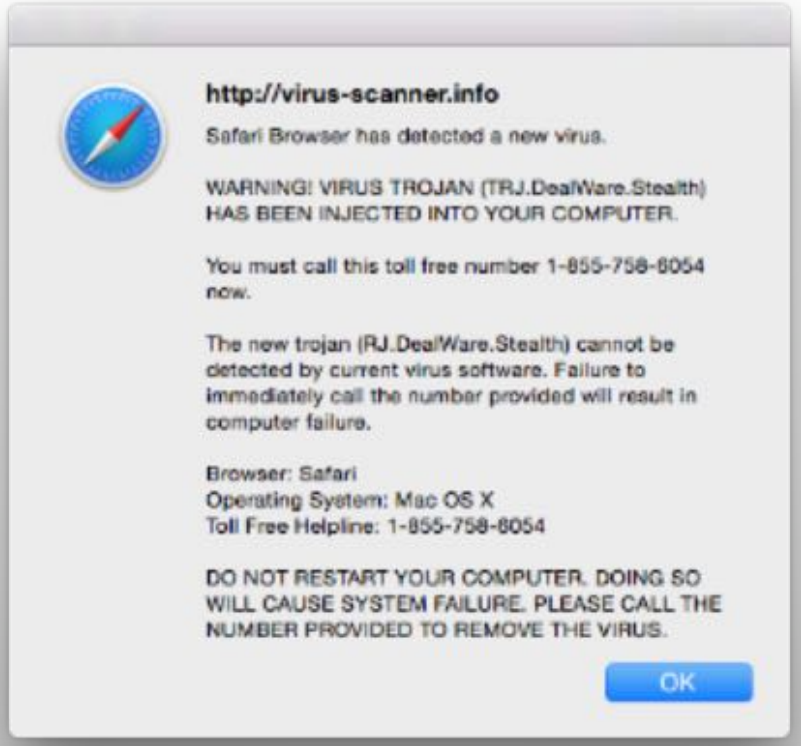
- Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system.
  - Could be Virus
  - Could be designed to use your Mac to spam others or attack servers as a “bot”
  - Could be a ”PUP” Potentially Unwanted Software
  - Could be Spyware
  - Could be Adware

  - But before we discuss the above real issues it could be……

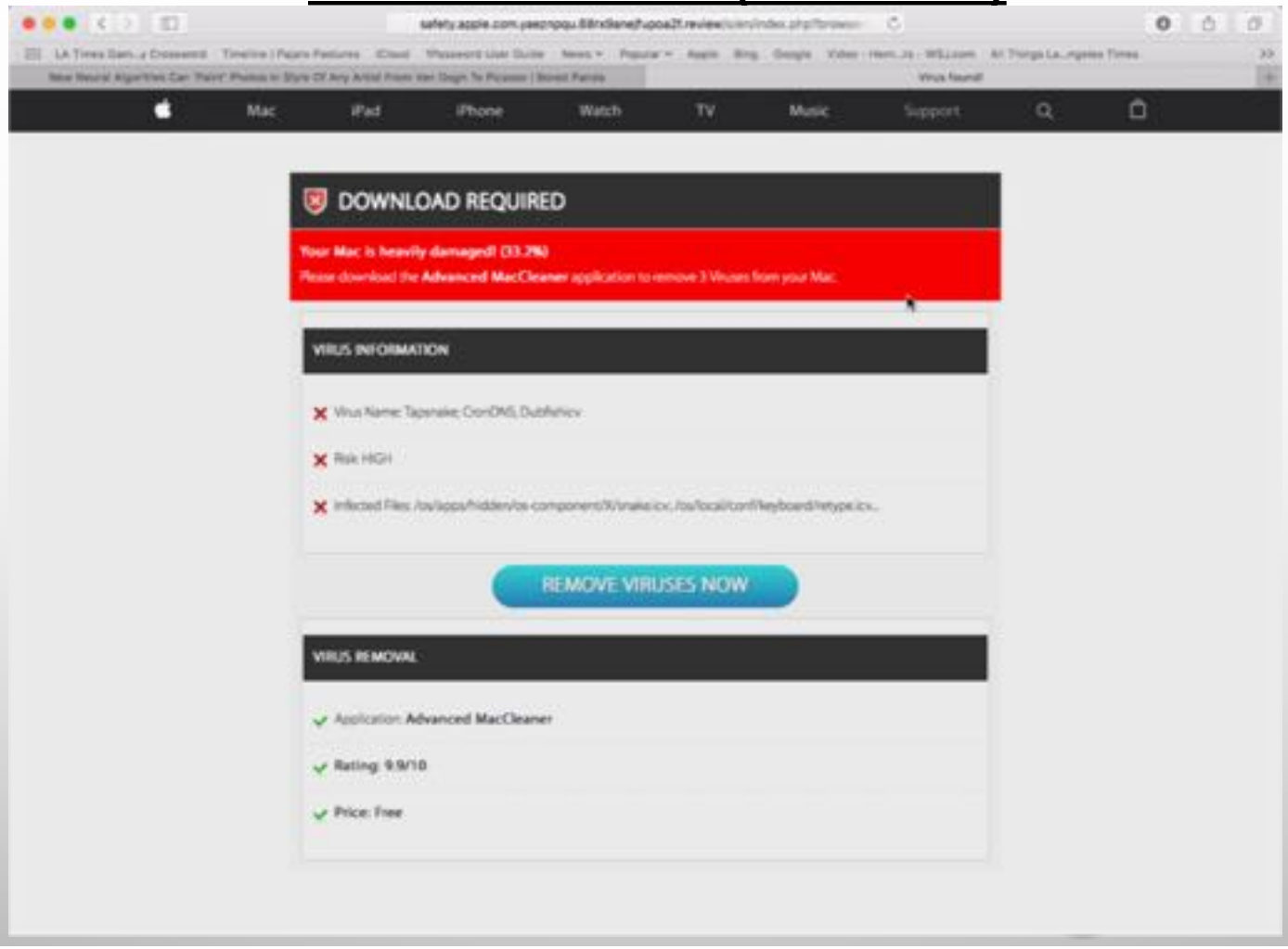
VIRUS SCAMS

- You are surfing the Internet when a pop up window shows up and
  - We've scanned all your hard drives and you have 2,367 viruses!! Call 1-900-xxxx
  - Apple LLC or The Mac OS company has determined your Mac is infected and all accounts are suspended. Click here to download a remote access program and you will be contacted by…
  - Homeland security has detected a National threat to our nation caused by your Mac. This notice had personally been reviewed by both the President and Vice president. A swat team and 10,000 marines will be outside your house if you don't respond within 30 seconds…..
  - Awful danger sounds are coming from your Mac speakers….
- THIS IS A SCAM FOLKS>>> NOT REAL
- Just QUIT YOUR BROWSER… and move on.
- BUT you may not be able to quit. The web page is using javascript to block things and/or launch more pop up pages. You get told your computer will send out a death ray through the walls and kill your dog (and you don't have one)

VIRUS SCAMS (CONT'D)



VIRUS SCAMS (CONT'D)



VIRUS SCAMS

- How to get out if quit won't work:
  - Force Quit Safari (or other browser) (CMD-OPT-ESC)
  - Hold down the shift key and restart your browser. This will prevent the same page from reloading.
  - Go to the Safari Menu and CLEAR HISTORY and WEBSITE data. May be in a different location in other browsers.
  - If you are still stuck turn off WI-FI or pull the Ethernet cable from your computer to disconnect from the internet. Re launch your browser. You will get a message "you are not connected to the internet" Go to preferences and change your homepage back to what you previously had. Reconnect to the internet and you should be back to normal.
  - NEVER CALL THE NUMBER-they will have you install a remote access program and install whatever they want. They will charge your credit card for this scam, and then may "sell the credit card info to a friend"
  - Remember almost always there is no way to have a external website look at the contents of your mac and it will take time to examine your hard drive for malware.

MALWARE-VIRUS

- This may be the hardest slide to create. Seems there are many conflicting definitions.
- For the purposes of this presentation we are only talking about Mac Viruses.
  - We will not be discussing Windows, Android or pre OSX Mac Viruses.
    - Modern Intel Macs can't get these.
- I'll limit the definition to self replicating code attached to files or programs designed to create harm on the Macintosh hardware and Operating system.
  - Rarely will the virus announce itself. The Southwest airlines Pink Slip Virus commercial of 2007 (need to get away) was probably 10 years out of date then.
  - I'm going to ignore things like Microsoft Word Macro Viruses. Apple Pages and Openoffice that can read Word files do not execute macros, so the problem is only confined to Word users or perhaps another program that can execute Word macros.
    - Only advise here if you use Word is to keep it up to date and do not enable macros from files you get from the Internet, unless you are 100% certain you need to.
- These viruses often used to attack specific memory locations on you machine to cause harm. This type of attack mostly been thwarted. More later.

MALWARE-VIRUS (CONT'D)

- There was big story back in 2012 about the Flashback virus.
  - Indications were that the original version was a Trojan (posing as Adobe Flash Installer)
  - Later versions could self replicating.
- Flash Back took advantage of a flaw in JAVA language installed on Macs at that time to install itself.
- This is largely a past problem. Apple addressed this virus directly, and later versions of JAVA did not have the flaw.
  - JAVA is no longer installed into the Mac OS
- From what I have read there is not a lot Malware in the form of a classic virus.
  - It seems many Anti-virus programs concentrate on finding an eliminating Windows based virus's and this type of Macintosh virus's.

MALWARE-SPAM & BOT TYPES

- The assumption is that Malware exists solely to harm a victims Macintosh. Not always the case.
- There is malware that will send out SPAM emails to those on your contact list or lists obtained from a rogue site. The program will either keep the number of emails down to some number (~100) that will not trigger immediate shutdown of your mail account, or if an open port is present will use your Mac as a open mail server and send as many as possible till your ISP shuts your account down.
- Bot malware is short for BOTNET malware. A central bad actor will use thousands of similarly compromised machines to "attack" a specific website. Leo Laporte use to give an example of a off shore betting website. In a Mafia Don accent, he would say "It would be most unfortunate if your servers were hit with denial of service in the days leading up to the Superbowl" ie pay up now or face the consequences.
- Will slow down your Mac for sure, and I've mentioned the ISP consequences.
- In my opinion I would think the Malware authors will concentrate more on IOT devices

MALWARE-PUPS

- PUPs is Potentially Unwanted Programs. It is overly simplistic to merely label these types of programs as scams, that do more harm than good. Many are but..
- There is a big market for Parental Control software designed to monitor your Kids (grandkids) internet usage, block bad sites, vulgar words etc. If you are a kid this is definitely unwanted software! (This software will let the Kid know they are running, it is just that the Kid's non-admin account can't remove it) Note that there would be legal issues for Anti-Virus programs to directly remove these programs from a Mac.
- Then there are some bad actors like Mackeeper and TuneMyMac, Machshiny that while the may due a few things are:
  - Unethically marketed (had fake websites on typos of other vendors urls)
  - Fake positive reviews
  - Creates system Instability
  - Performance hit
  - seems to use adware advertising

MALWARE-PUPS (CONT'D)

- Avoid getting "cleaner" and "Optimizer" programs in general. NOT NEEDED.
- Marginal at best, mostly Scams.
- Malwarebytes will identify some of these programs and give you the option to remove them.

MALWARE-SPYWARE

- As a blues fan, I know of songs by Muddy Waters, Koko Taylor, and Otis Spann had song lyrics with the phase "Another Mule Kicking in my Stall" ie Adultery.
- So there is software out there to log keystrokes and stay hidden so you can spy on your Spouse. I does not take much imagination to see that other bad folks could also install such software on your Mac.
- If through the internet, say by phishing; they get you to install it, and their goal is not your personal issue, but getting bank and other financial information.

MALWARE-ADWARE

- Adware was the main topic of my previous presentation.
- Yes there is some advertising supported legitimate software where you choose to see ads instead of paying for program. However this is an exception now.
- There is lots of Malware that is adware.
  - Displays Advertisements where non should exist (Note there are plenty of websites with Ads, some even with pop up ads) For example space.com has ads on the side and will have a one time pop up touting the advantages of a subscription to the site. Pop up by pop up would not be expected behavior.
  - Likewise an Adult ad in the Elementary school volunteers timesheet would most likely be adware. Or tons of pop ups on the ticket ordering website when you have only 30 seconds left before they cancel your order because you still can't locate your credit card!
- Changes your homepage
- Changes you preferred search engine

MALWARE-ADWARE (CONT'D)

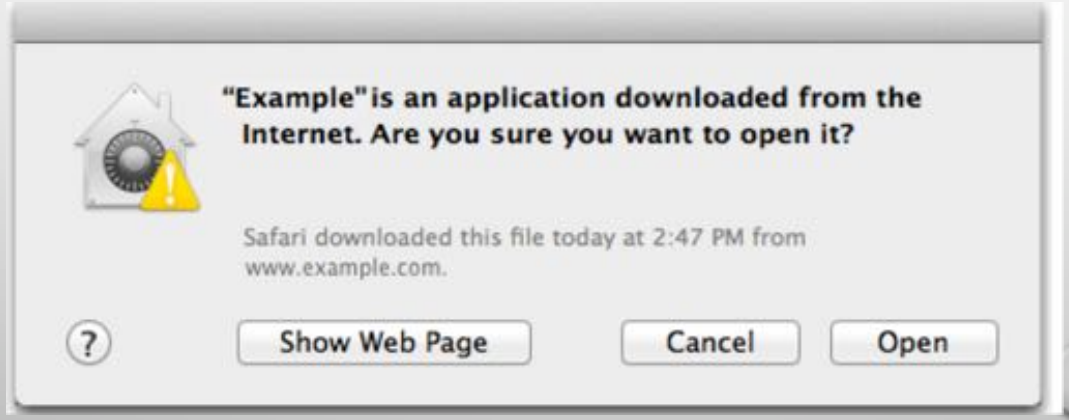
- Some of this may be the unintended consequence of Ad blockers.
- Seems to be a growing concern.

MALWARE-APPLE'S DEFENSES

- I sometimes read how Apple computers have no defense against Malware
  - Often from Anti-Virus companies, leads one to question the rest of their claims!
- Address space layout randomization (ASLR) introduced in OS X 10.5 leopard and improved in OS X 10.7 Lion.
  - Prevents an attacker from jumping to a particular exploited function in memory by randomly arranging address space positions.
- Gatekeeper- Introduced in OS X 10.7.5. Gives you control over what gets installed.

MALWARE-APPLE'S DEFENSES (CON'TD)

- Earlier versions of Gatekeeper did have an option to open anything. Not recommended.
- Gatekeeper will also flag "damaged" programs that in reality were modified after the fact of being certified.
- XPROTECT- introduced in OSX 10.6 Snow Leopard.
  - Works with Mail, Safari, iChat and Messages.
  - Runs in the background checks against major malware (not all), no user intervention
  - Gets periodic updates from Apple
- Xprotect Dialog:
-



MALWARE-APPLE'S DEFENSES (CON'TD)

- If you did not knowingly download something HIT CANCEL
- Xprotect Dialog box for malware downloads it detected:

- Of course you want to MOVE TO TRASH.
- What about those fake dialog boxes examples earlier in the SCAM section. Use common sense; would a Malware Author give you this option?
- https://support.apple.com/en-us/HT201940

MALWARE-HOW TO STAY SAFE

- "Jim What is the magic bullet antivirus software to keep me 100% safe?" I already answered this in the second slide. DOES NOT EXIST.
- Malware will often exploit security issues in operating systems, programs, browser extensions, etc.
- For the Mac OS operating system Apple is only patching the following
  - OS 10.13 High Sierra
  - OS 10.12 Sierra
  - OS 10.11 El Capitan
- Go to preferences > APP STORE and at least have Check for updates and system data files install checked [DEMO]
- Have your programs autoupdate or if they don't have it check for updates. Examples Microsoft Office 2016 (monthly), 1Password etc.
- Three items to call out JAVA, Adobe Flash, and Adobe Reader.

MALWARE-HOW TO STAY SAFE (CONT'D)

- BACKUPS!
- Yes SBAMUG and countless others have been constantly preaching about backups. When not if your hard drive fails… Do you want to loose your Tax records and photos of the grandkids? Important points
- But some Malware is poorly written and even if it is not the intent, the Mac OS, programs, or data files could be damaged. How do you recover > Backups.
- Ransomware… Have not really mentioned this before. Does exist. Fair amount is just a SCAM to extract money, but some programs are real. If you are not informed in time by Xprotect or other solutions, it is possible to have your hard drive encrypted. Paying the ransom is expensive, encourages the bad guys to continue, and it still may not be possible to unencrypt your hard drive. If you are following a good backup practices you will have an offsite backup that is not a regular (daily) part of your backup. The good ransomware programs will given time also encrypt your external backup drives. The offsite one will save you!

MALWARE-HOW TO STAY SAFE (CONT'D)

- The REAL PROBLEM IS YOU!!!!
- Any software solution depends on catching Malware quickly. If its of the Adware type, it is a pest remove it, and carry on. If it is nasty, and you were tricked to downloading and installing it, it may be too late. YOU DID IT TO YOURSELF!!
- Let start with the Software download aggregator websites. If you are Adobe or Microsoft your marketing budget allows magazine ads, billboard, TV commercials and in the past big kiosks in software stores. What if you are a one man shareware author. How do you let folks know about your product? There still are the aggregator websites. Today 22 new shareware programs. Yours is there with reviews and the ability for anyone to download from the sites servers. Plenty of Ads in the sidebars and if you were say Intuit your latest version of Quickin would show up with big color fonts surrounded by a banner. For a fee of course. Everybody was happy..

MALWARE-HOW TO STAY SAFE (CONT'D)

- But then something happened to several of these sites. They turned EVIL!! Whether it was just greed or the Advertisers refused to pay the same rates due to adblockers, I don't know. Hey if you bundle Mackeeper with the download and really make it hard to tell, $0.75 or whatever per download goes into your sites account. Easy money.
  - Softonic
  - Cnet's Download.com
  - MacUpdate (last big one)
- So avoid downloading from these sites. I guess you can still use them to see what is new, but go directly to the Shareware authors site and download from there!
- The issue is that just avoiding these three is no guarantee. Are there others, or maybe some site with out of copyright free games out there that is also evil? Do you think I have the time to go to every site on the entire internet and find them???

MALWARE-HOW TO STAY SAFE (CONT'D)

- Finally you may get tricked without going to a known bad website.
- Lets me go through this excellent Apple support DOC line by line with you:

- https://discussions.apple.com/docs//DOC-7471
- Get the Idea?

- Okay you see video link online and it is of your favorite Singer/Actor/Sports team/whatever. Preview/and or Quicktime can't open it per a legitimate Mac OS dialog box. Have you gotten VLC? If it can't open it, in my opinion the site is too stupid to be on the Internet. However you may get:
  - You Need to get the XXXX,YY Codec to view this
  - OR Your Adobe Flash is out of date. (and you don't have Flash installed or just updated it 5 min ago!)
- Guess what this is either a trick to get Windows users infected, or perhaps the link server sees Browser= Safari Machine=Macintosh and downloads Mac Malware to YOU!!

MALWARE-HOW TO STAY SAFE (CONT'D)

- Decide if you need Adobe Flash. If you have it this is how to update:
-

- Don't have it go to Adobe.com and get it. Not from pop up or email.
- The above bullet applies to other programs as well. Go to the website if there is no built in updater.
- Of course avoid pirate sites and even torrent sites can be high risk.

MALWARE-SOME RECOMMENDED PROGRAMS

- There are two programs Malwarebytes for Mac and Etrecheck
- Malwarebytes:
  - Started as donationware Adware Medic for the Mac
  - The Malwarebytes.org organization purchased the program and kept the Author on staff
  - Since has evolved; scan part free, Active real time protection is annual subscription
  - Aimed at Mac Malware, no windows malware scanning
- Etrecheck:
  - Started out as a program for knowledgeable folks on Apples community discussion boards to accurately understand what was going on with the questioners mac.
  - Mac Model, Ram, installed programs, start up items, background items etc, with personal information removed is summarized into a list to be attached to the board.
  - They soon discovered the many had adware and the like.
  - Later versions are more specific to this Malware/Adware, and give a choice to remove it.

  - I'll go to both websites.

MALWARE-FULL ANTIVIRUS PROGRAMS

- There are lots of full up comprehensive Antivirus programs.
  - Norton Antivirus
  - Sophos Home Premium
  - Trend Micro
  - Intego Mac Internet Security
  - McAfee
  - Avast
  - BitDefender
  - ClamXav
  - Kaspersky
  - MacScan3
- Kaspersky is prohibited in Government use due to its companies ties to the Russian government.
- CleanMyMac - "another victim" per a quote from Apple's discussion boards on the problems he was having with his Mac; it was later determined he had installed this

MALWARE-FULL ANTIVIRUS PROGRAMS (CONT'D)

- Norton was crashing my PPC Mac daily till I uninstalled it. May not be relevant to today's version but..
- I still have ClamXav. Used it to check the shareware programs I would burn onto CD's for the PD CD. We no longer offer the CD. Okay with the program when it was donationware, I'm less likely to recommend it today now that it is a paid version.
- I suppose if you deal with Windows files one could make more a case for these programs.
- Many of these programs do all sorts of things.
  - Checking your Mail may be fine, but most ISP's check for Malware and phishing
  - Cache cleaning may occasionally help, but constant cleaning of caches will slow down your machine, that's why they exist.
  - Safari has good tracking cookie prevention now. Deleting all cookies can create issues on Websites that use them to validate you.

MALWARE-FULL ANTIVIRUS PROGRAMS (CONT'D)

- Some were thinking the "Pro" not customer versions of Anti-Virus would be better
  - Not applicable to home use, due you have a dedicated server(s) machines and are an expert network admin?; didn't think so.
- Bear in mind that sometimes these programs think they see malware type activity that is actually some Mac OS system routine, remove it, and that can cause a lot of problems. (heuristic)
- Finally let me show you the final thought on Antivirus programs from this support document:
- https://discussions.apple.com/docs/DOC-8841

MALWARE-CONCLUSION

- The operator behind the Keyboard is the best resource for dealing with Malware. Stay patched. Think before downloading things.
- QUESTIONS?