Protecting Your Mac

Antivirus and Anti-Malware Applications

SMMUG Presentation

Do We Really Need To Have Protection?

- Why? I've never needed it before!
- I thought Macs were impervious to viruses
- That's why I use Macs and don't use Windows
- What's changed? Has the environment gotten worse?
- What could possibly go wrong?

Some Good News

- Macs are more secure than their Windows counterparts
- OS X is a Unix-based operating system so it is sandboxed. It's like having a series of fire doors - even if malware gains access to your Mac, it is unable to spread to the heart of the machine
- Macs are not unhackable, but they are more difficult to exploit than Windows PCs
- Malware writers are less likely to target Mac users because of the perception that it has a far smaller market share than Windows
- Apple has included a number of security measures that make attacking a Mac particularly challenging. These include Gatekeeper, which blocks any software than hasn't been digitally signed and approved by Apple from running on your Mac without your agreement

The World Has Changed For The Worse

- In 2012, there was the Flashback Trojan that infected 600,000 Macs
- In 2013, a targeted attack hit OS X developers at Microsoft, Facebook, Twitter and Apple itself
- In 2015, the XcodeGhost attack poisoned hundreds of OS X and iOS apps
- In early 2016, the first known piece of encrypting ransomware for Macs appeared

Definitions

- **Virus:** A program designed to copy itself and propagate, usually attaching itself to applications. It can be spread by downloading files, exchanging CD/DVDs and USB sticks, copying files from servers, or by opening infected email attachments
- **Worms:** A worm can be injected into a network by any types of means, like an USB stick or an email attachment. Email worm tends to send itself to all email addresses it finds on the infected PC. The email then appears to originate from the infected user, who may be on your trusted senders' list, and catch you off guard
- **Trojan:** It might appear harmless and even useful at first, but it leaves your PC unprotected, enabling hackers to steal sensitive information
- **Spyware:** Often secretly installed without consent when a file is downloaded or a commercial pop-up is clicked. Spyware can reset your auto signature, monitor your keystrokes, scan, read and delete your files, access your applications and even reformat your hard drive. It constantly streams information back to the creator of the spyware
- **Adware:** This malware launches advertisements, mostly in the form of pop-ups. These are customized to you as a user, based on your behavior on the Internet, which may be monitored by spyware

Definitions Continued

- **Spam:** Unwanted emails. Most users are exposed to spam, which is more than 50% of all Internet emails. Though spam is not a direct threat, it can be used to send different kinds of malware
- **Phishing:** The fraudulent acquiring of sensitive personal information such as passwords and credit card details. This is accomplished by sending official-looking emails impersonating a trustworthy sender. Users of online banking and auction sites are most likely to become a target
- **Pharming:** A more sophisticated form of phishing. By exploiting the DNS system, pharmers can create a fake website that looks like a real one for instance web bank page, and then collect the information users think they are giving to their real bank
- **Keyloggers:** Designed to record the user's keystrokes. Keylogging allows criminals to look for particular bits of information that can be used for identity or intellectual property theft
- **Rogue security software:** A special type of threat is software that claims to be security software. It tricks users that have installed it to pay a sum of money to be really protected (which they will not be). Most often it pretends to be antivirus and antispyware programs

Ransomware

- A sub-category of malware that involves software sneaking itself onto your computer and then encrypting files. You'll be left with two options: never be able to access those files again, or pay the 'ransom' to decrypt them
- For a long time ransomware was a problem that Mac owners didn't have to worry about, but March 2016 saw the appearance of the first Mac ransomware - KeRanger, distributed along with a version of a piece of legitimate software: the Transmission torrent client

What are the symptoms of a computer virus?

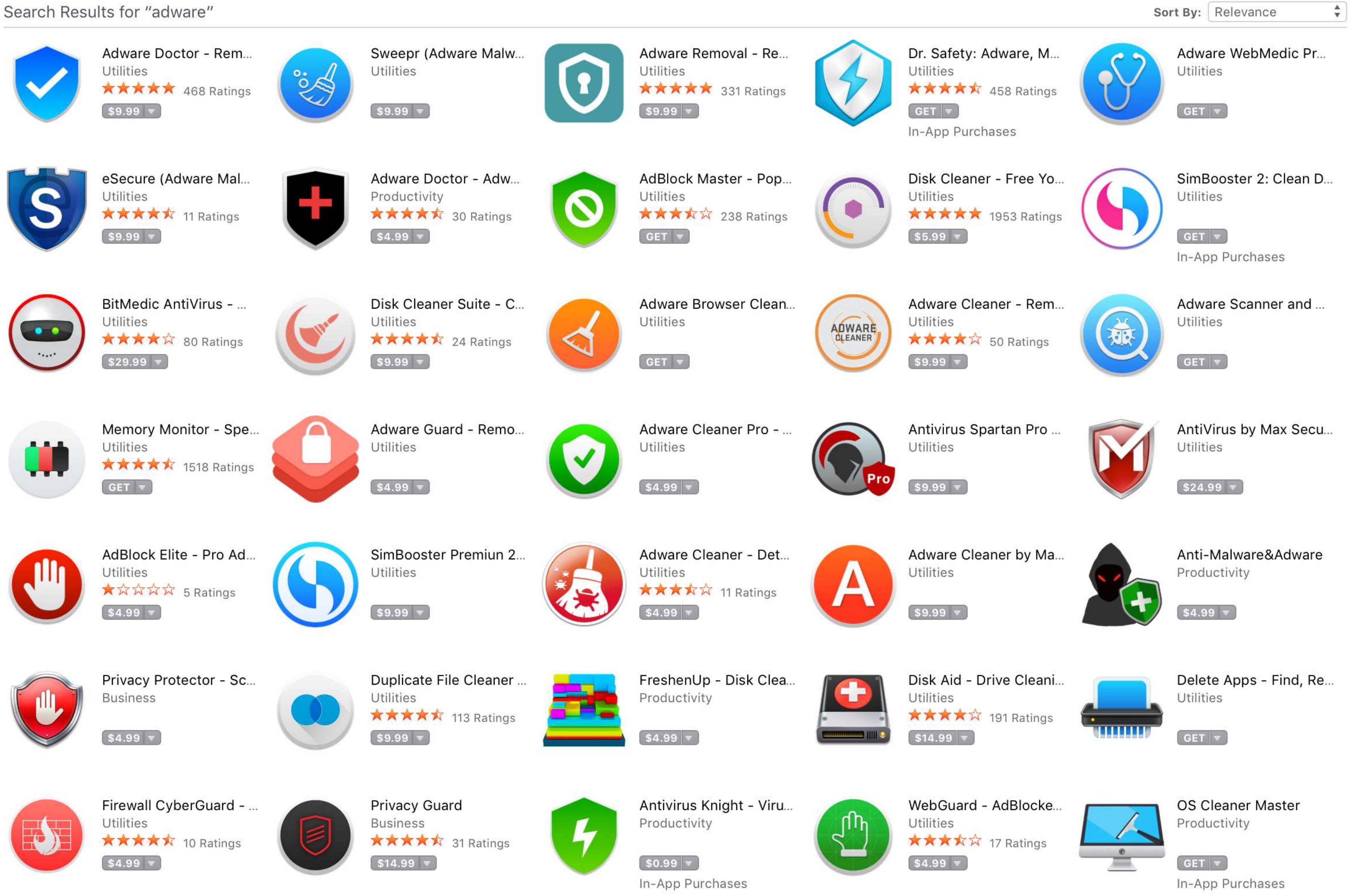
Your computer may be infected if you recognize any of these malware symptoms:

- Slow computer performance
- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes

What Can You Do?

- Make sure that you have security software on your Mac
- Use antivirus software
- Get antispyware software
- Always keep your antivirus protection and antispyware software up-to-date
- Update your operating system regularly
- Increase your browser security settings
- Avoid questionable Web sites
- Only download software from sites you trust. Carefully evaluate free software and file-sharing applications before downloading them

What’s Available on the Apple Store?



Search Results for “adware”

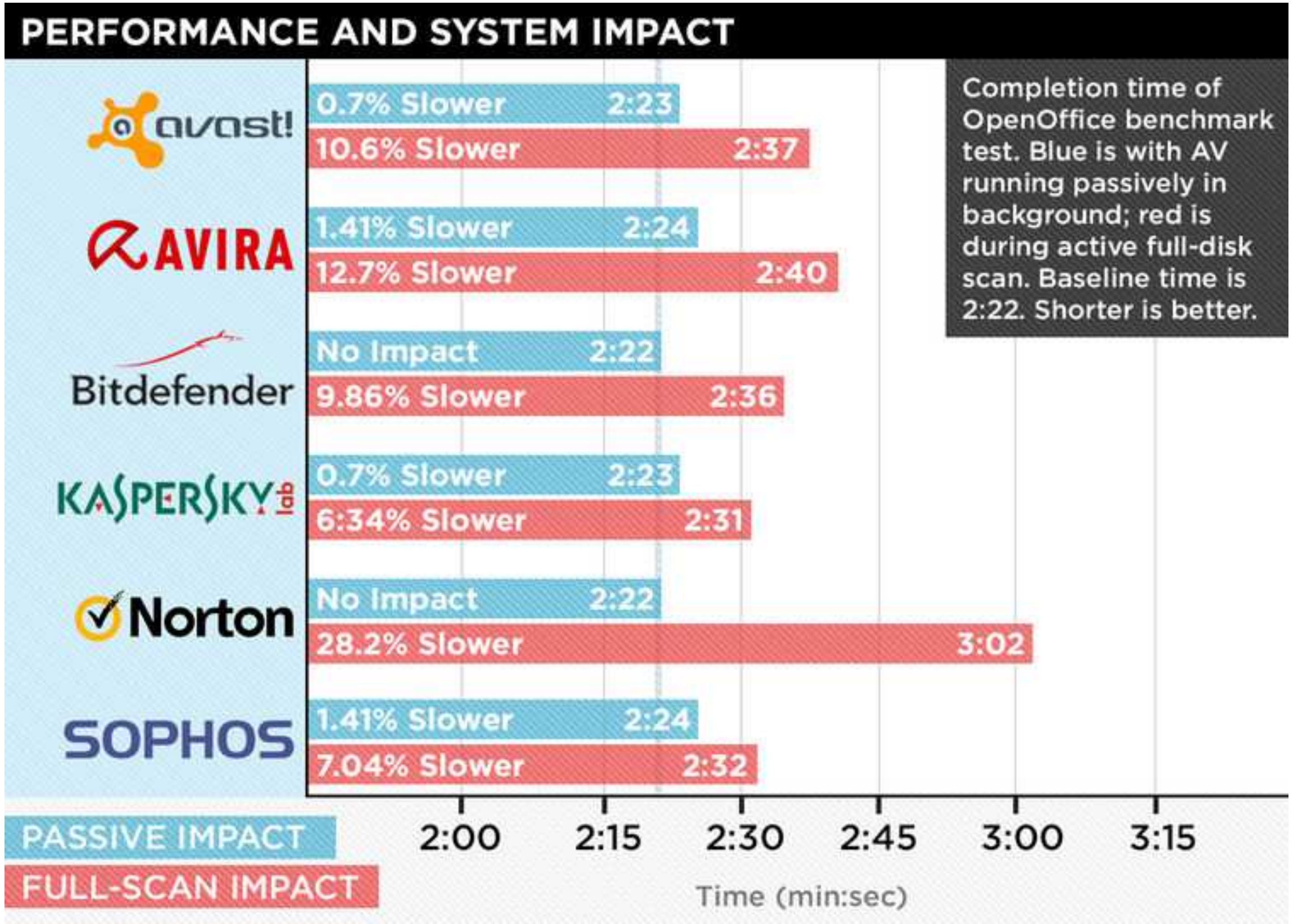
Sort By: Relevance

Adware Doctor - Rem... Utilities ★★★★★ 468 Ratings $9.99	Sweepr (Adware Malw... Utilities $9.99	Adware Removal - Re... Utilities ★★★★★ 331 Ratings $9.99	Dr. Safety: Adware, M... Utilities ★★★★☆ 458 Ratings GET In-App Purchases	Adware WebMedic Pr... Utilities GET
eSecure (Adware Mal... Utilities ★★★★☆ 11 Ratings $9.99	Adware Doctor - Adw... Productivity ★★★★☆ 30 Ratings $4.99	AdBlock Master - Pop... Utilities ★★★☆☆ 238 Ratings GET	Disk Cleaner - Free Yo... Utilities ★★★★★ 1953 Ratings $5.99	SimBooster 2: Clean D... Utilities GET In-App Purchases
BitMedic AntiVirus - ... Utilities ★★★★☆ 80 Ratings $29.99	Disk Cleaner Suite - C... Utilities ★★★★☆ 24 Ratings $9.99	Adware Browser Clean... Utilities GET	Adware Cleaner - Rem... Utilities ★★★★☆ 50 Ratings $9.99	Adware Scanner and ... Utilities GET
Memory Monitor - Spe... Utilities ★★★★☆ 1518 Ratings GET	Adware Guard - Remo... Utilities $4.99	Adware Cleaner Pro - ... Utilities $4.99	Antivirus Spartan Pro ... Utilities $9.99	AntiVirus by Max Secu... Utilities $24.99
AdBlock Elite - Pro Ad... Utilities ★☆☆☆☆ 5 Ratings $4.99	SimBooster Premiun 2... Utilities $9.99	Adware Cleaner - Det... Utilities ★★★☆☆ 11 Ratings $4.99	Adware Cleaner by Ma... Utilities $9.99	Anti-Malware&Adware Productivity $4.99
Privacy Protector - Sc... Business $4.99	Duplicate File Cleaner ... Utilities ★★★★☆ 113 Ratings $9.99	FreshenUp - Disk Clea... Productivity $4.99	Disk Aid - Drive Cleani... Utilities ★★★★☆ 191 Ratings $14.99	Delete Apps - Find, Re... Utilities GET
Firewall CyberGuard - ... Utilities ★★★★☆ 10 Ratings $4.99	Privacy Guard Business ★★★★☆ 31 Ratings $14.99	Antivirus Knight - Viru... Productivity $0.99 In-App Purchases	WebGuard - AdBlocke... Utilities ★★★☆☆ 17 Ratings $4.99	OS Cleaner Master Productivity GET In-App Purchases

The Best Apps for Protection…

- …Aren't found on the App Store
- Plenty of good 3d party options available
- Free versus Paid
- Specific anti-malware, antivirus, anti-adware
- Consolidated products that incorporate all of the above
- You get what you pay for (free is not necessarily the best)

Analyses of Performance and Capabilities



PERFORMANCE AND SYSTEM IMPACT

Completion time of OpenOffice benchmark test. Blue is with AV running passively in background; red is during active full-disk scan. Baseline time is 2:22. Shorter is better.

- Various professional analyses show similar results
- Balance between cost, abilities, computer performance degradation
- Do your own due diligence
- Bitdefender had best performance (100% capture rate) and least degradation according to numerous analyses

Other Options Available

- MacWarrior 2
- ClamX AV
- Intego Mac Internet Security X9 (formerly VirusBarrier)
- Eset
- MacKeeper
- McAfee
- MalwareBytes
- Webroot

Conclusions

- We've gotten by without the need for security software until recently
- Most needed by high school and college students because of file sharing, bittorrents, surfing known dangerous sites
- Required by most universities
- There's also a "good neighbor" policy: You want to ensure that attachments sent from you (or especially forwarded from you) are safe and won't harm others' machines
- Keep your systems upgraded and current with security patches (Mac OS and iOS)