Craig Doran

- Solutions Team Manager/Architect at MacHero Inc. in Chicago Loop
- 14 years of professional Mac support. Mac owner since 1984.
- Previously a Risk Analyst and Safety Engineering consultant to Global 500 companies.
- Presenter at Society of Risk Analysis
- Apple, Casper, FileWave certified
- Suburban Chicago Apple Users Group - Technical SIG leader since 2010



Managing and User-Proofing Security as Malware Threat Grows

MACTECH PRO EVENTS

Bicycles for the Mind



- Fast at math(s)
- Never forget

Strengths of Modern Devices



- Great at encryption
- Great at maintaining data integrity
- Great at sharing data

Software Vulnerabilities

A vulnerability is any flaw that makes it infeasible, even when implemented or used properly, to prevent an attacker from; usurping privileges, regulating internal protected operations, compromising data, or assuming trust that was not explicitly granted.

Microsoft

Exploit

Exploits are the methodologies or techniques that are utilized to take advantage of vulnerabilities.

snort.org

Malware

Software that compromises the operation of a system by performing an unauthorized function or process.

https://niccs.us-cert.gov/glossary

Risk = Hazard x Exposure

Your level of risk is a product of your exposure to vulnerabilities.

Therefore you can reduce your risk by and/or:

1. **Reducing the vulnerabilities**
2. **Reducing your exposure**

Microsoft's Pre-Internet Legacy

- Windows struck early success in business
- Emphasized collaboration
- Did not transition well to the Internet age



Vulnerabilities in 2016

http://www.cvedetails.com/vendor-search.php

Vendor	Vulnerabilities	Source Model
Google	376	Open
Microsoft	266	Closed
Apple	234	Mixed

http://opensource.apple.com



Open Source	Closed Source
Open for all to review	Fewer eyes reviewing
Relies on voluntary reporting	Formal Quality Control
Free, so widely deployed	Restricted access

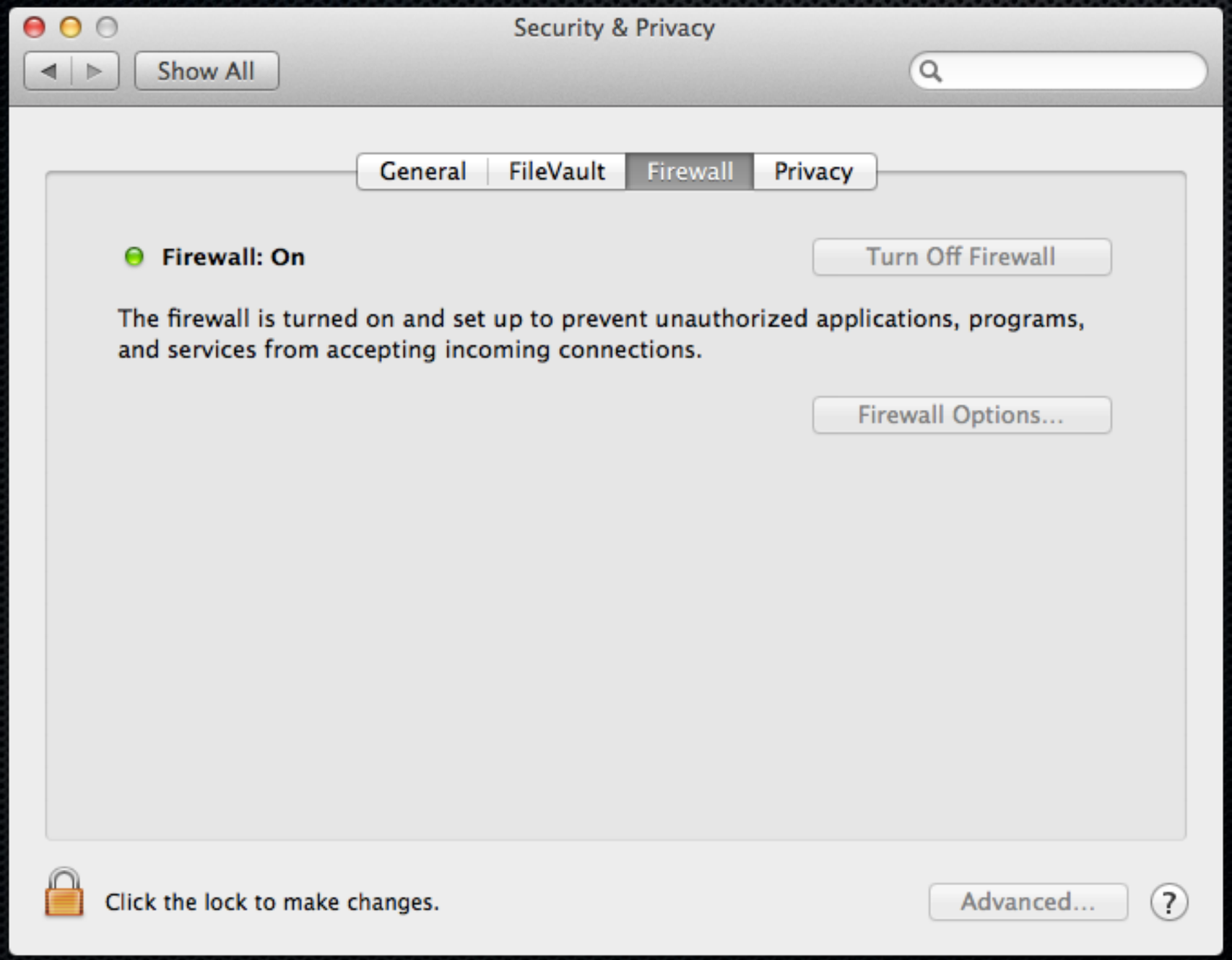
OS X Malware in 2016

- KeRanger ransomware
  - March
- EasyDoc Converter("Eleanor")
  - July

So how do we reduce the malware exposure for Macs?

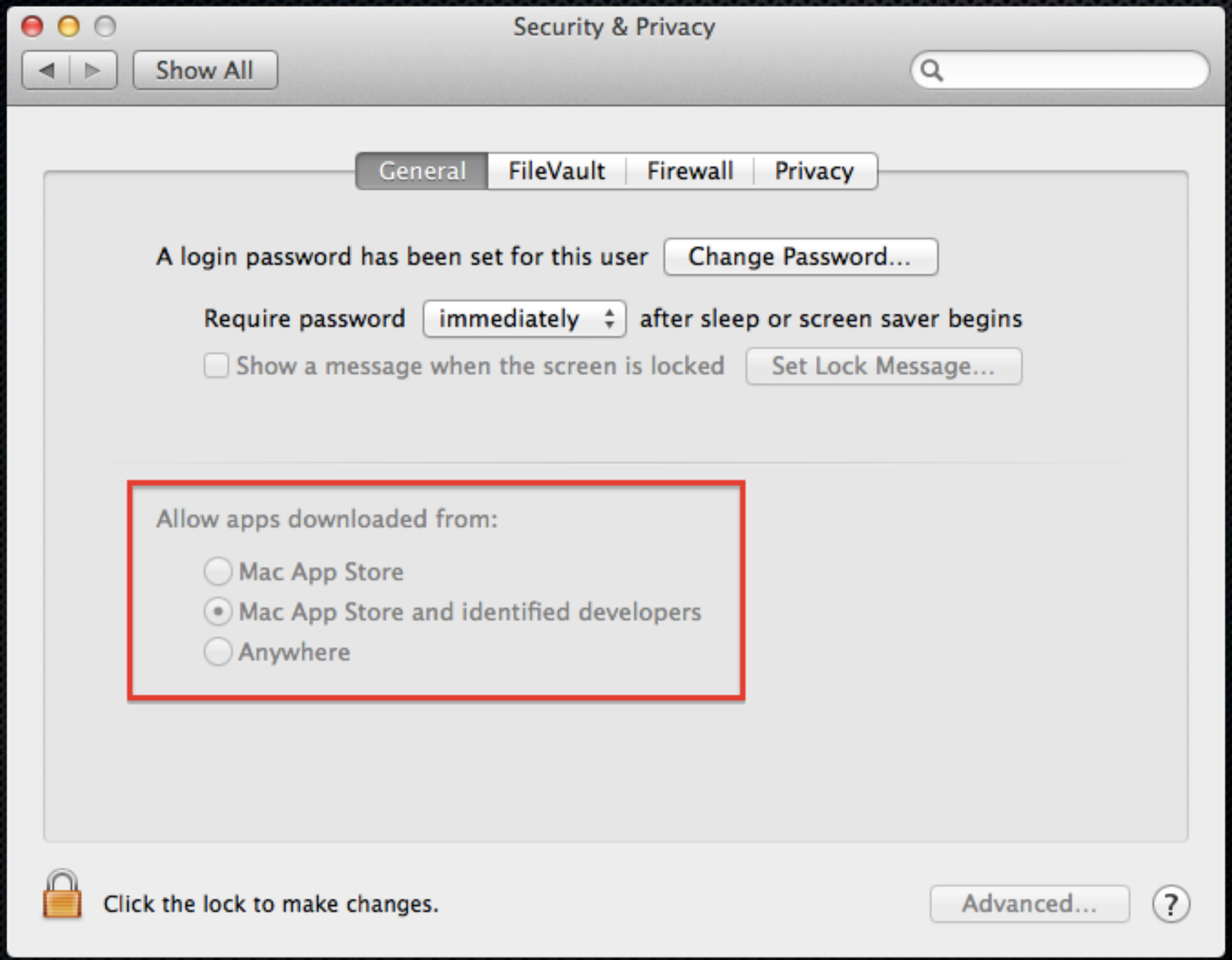
- Harden our systems
- Be aware of the vulnerabilities
- End User education

Basic OS X Hardening



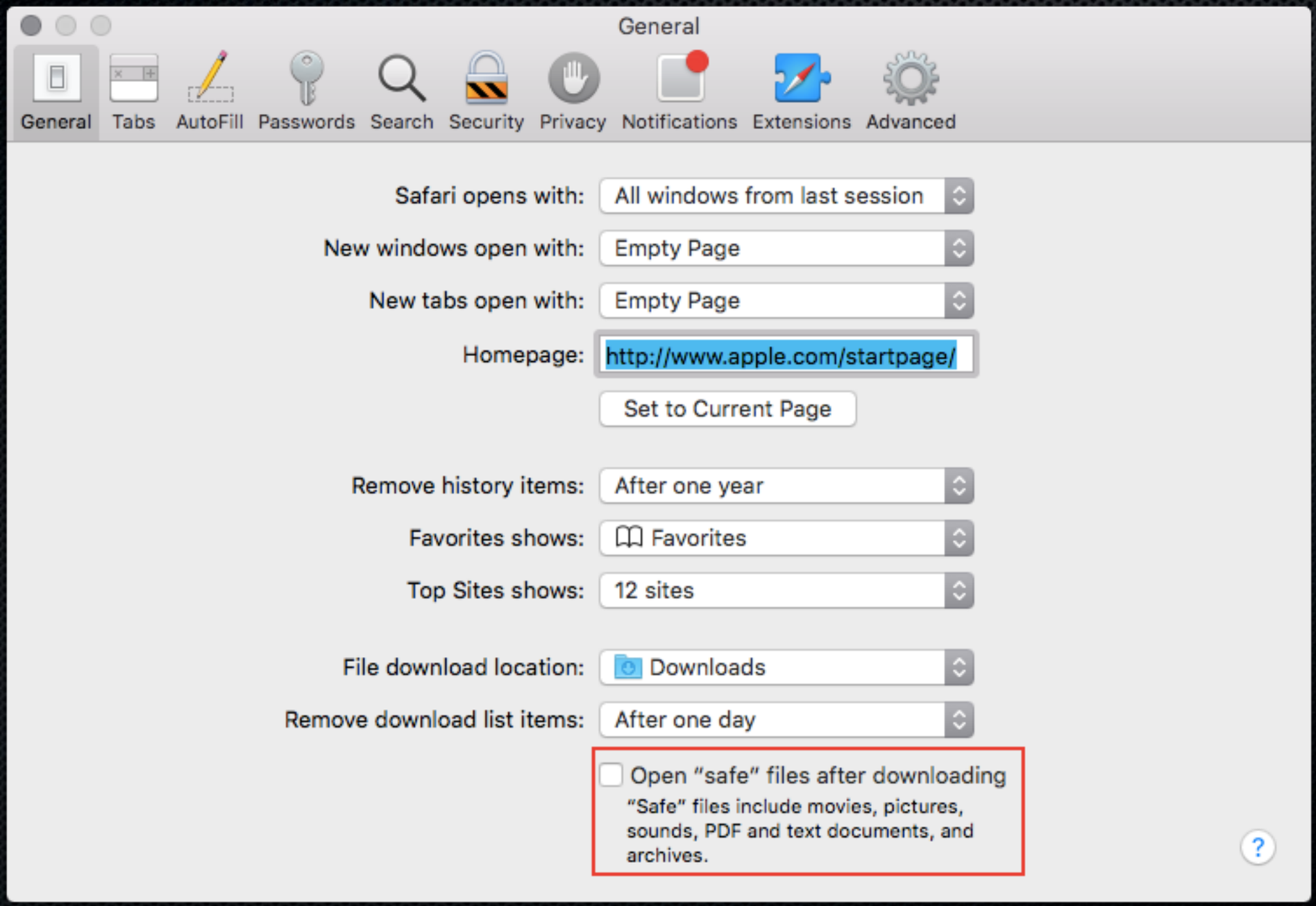
MACTECH

Basic OS X Hardening



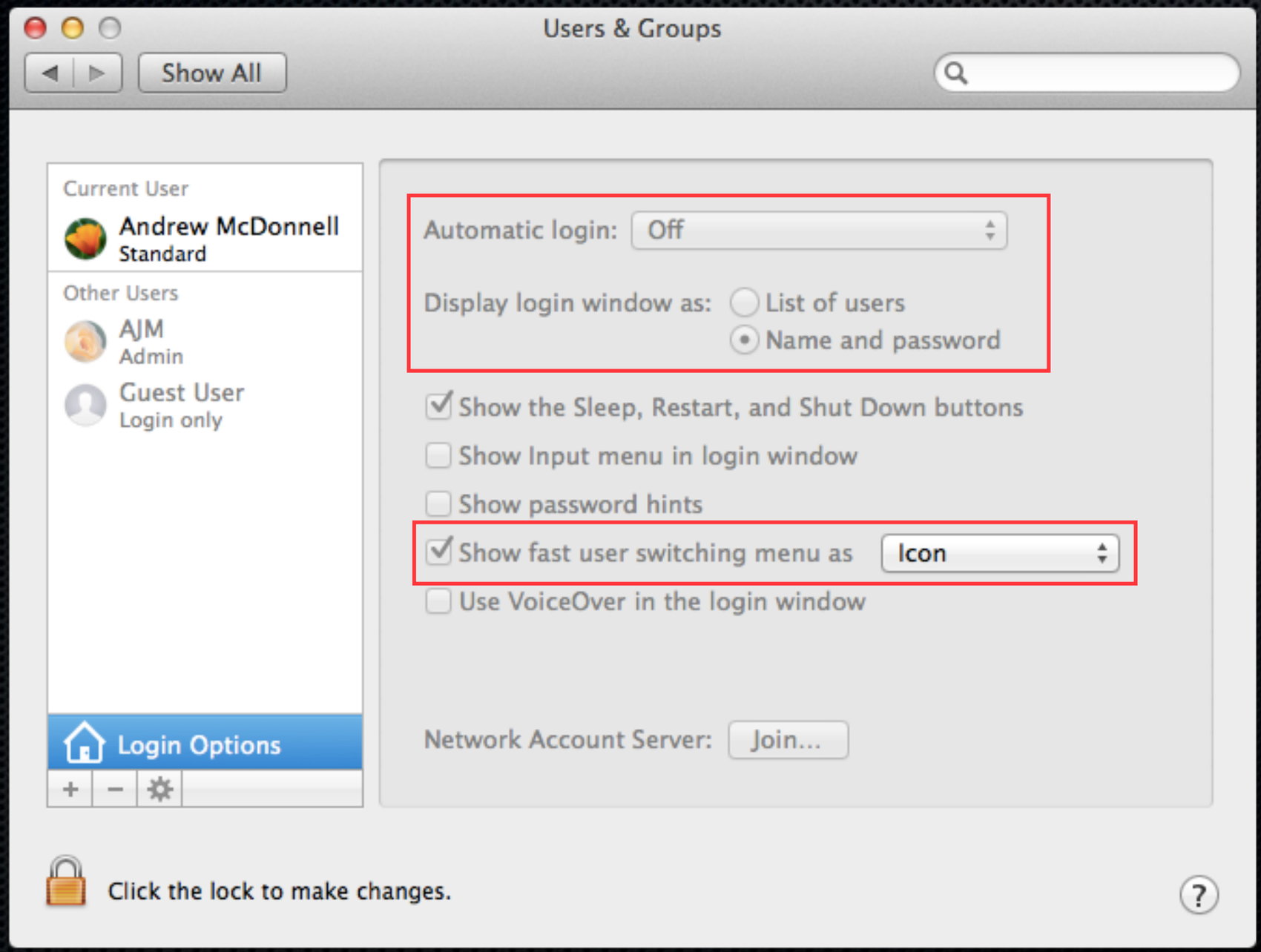
MACTECH

Basic OS X Hardening



MACTECH

Basic OS X Hardening



MACTECH

Stay Informed

- Apple Security Updates: HT201222
- http://www.thesafemac.com
  - https://blog.malwarebytes.com/author/treed/
- Vulnerabilities tracked at http://cve.mitre.org with unique CVE serial number.
- https://www.us-cert.gov

Malware Identification

- Anti-virus technology
- Advanced Threat Protection

Anti-Virus

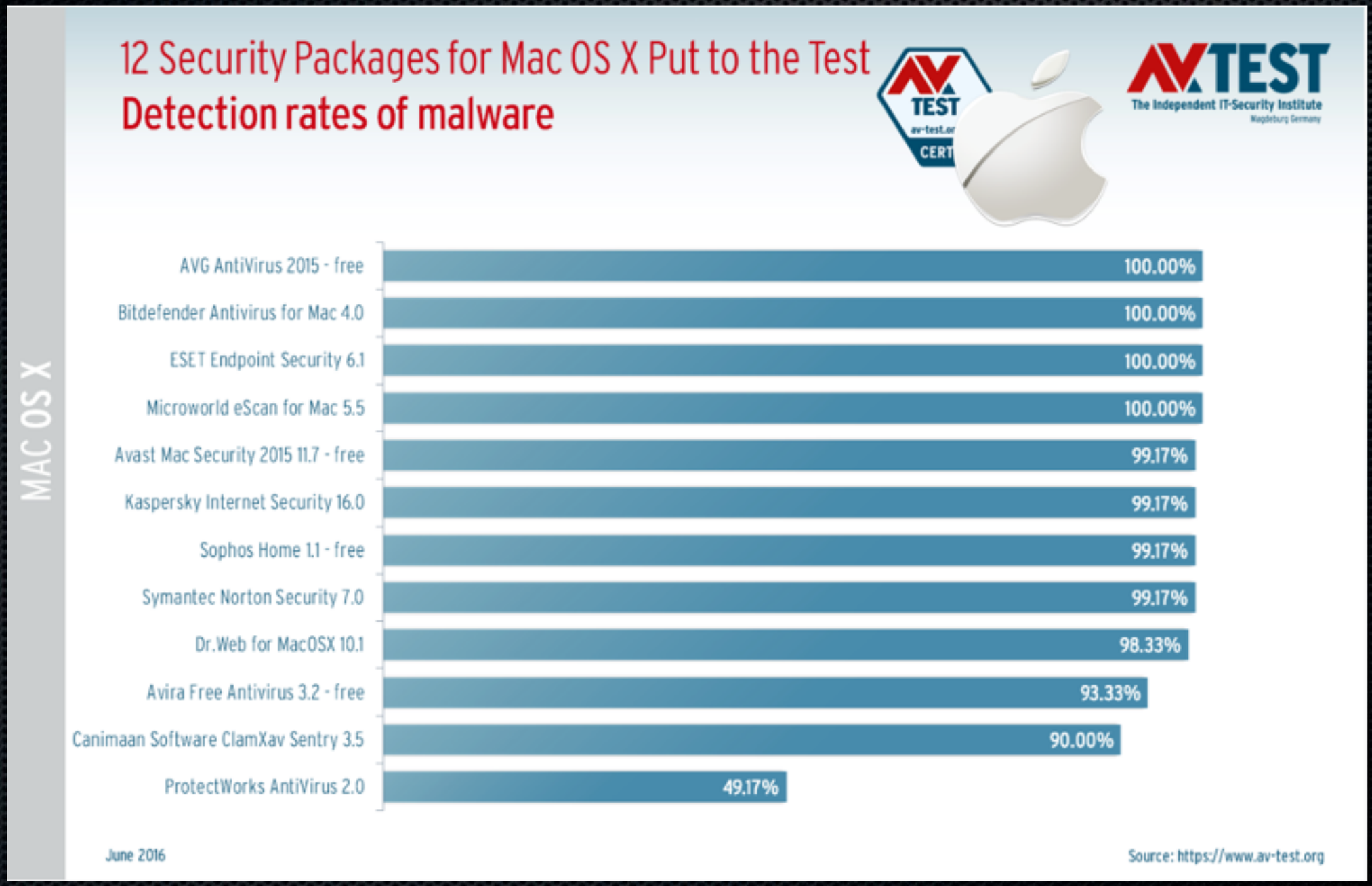
- Mechanism of Malware
  - Evildoers targeted popular legitimate software
  - Added their own launch codes to beginning of executable
    - Once the application launched, so did the nefarious processes
- Virus Scanners
  - Knew these prepended snippets of codes
  - Scan executables for these "signatures"

KeRanger

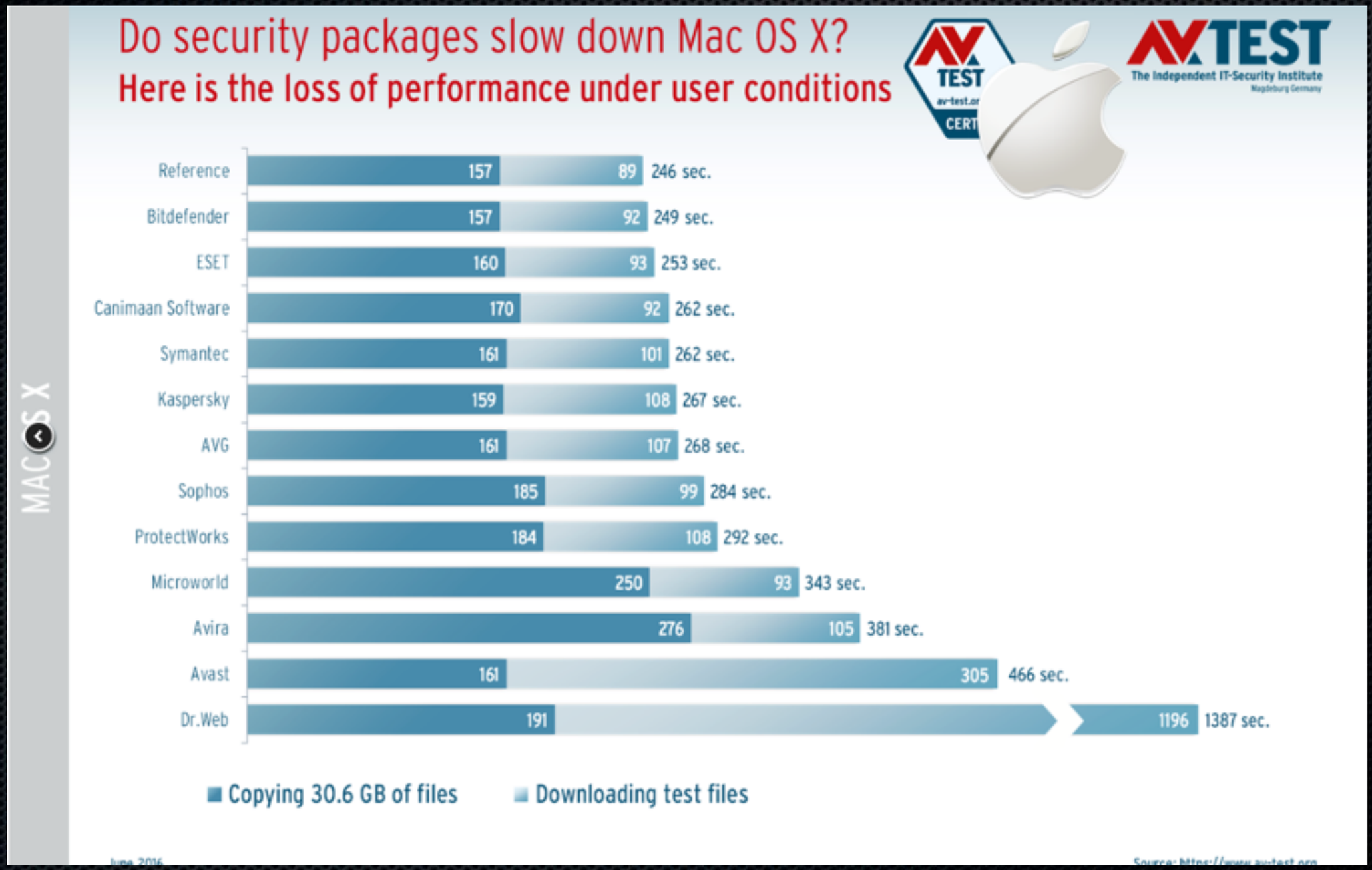
- Transmission BitTorrent client was infected.
- An executable .rtf is copied to ~/Library
- After 3 days Home and attached drives are encrypted



https://www.av-test.org



https://www.av-test.org



AV Selection Criteria

- Licensing
- Effectiveness
- Fewer side effects
- Mac knowledgeable
- Easily update definitions
- Passive on-demand vs. always active
- Centralized console
- Paid vs. Free

Advanced Threat Protection

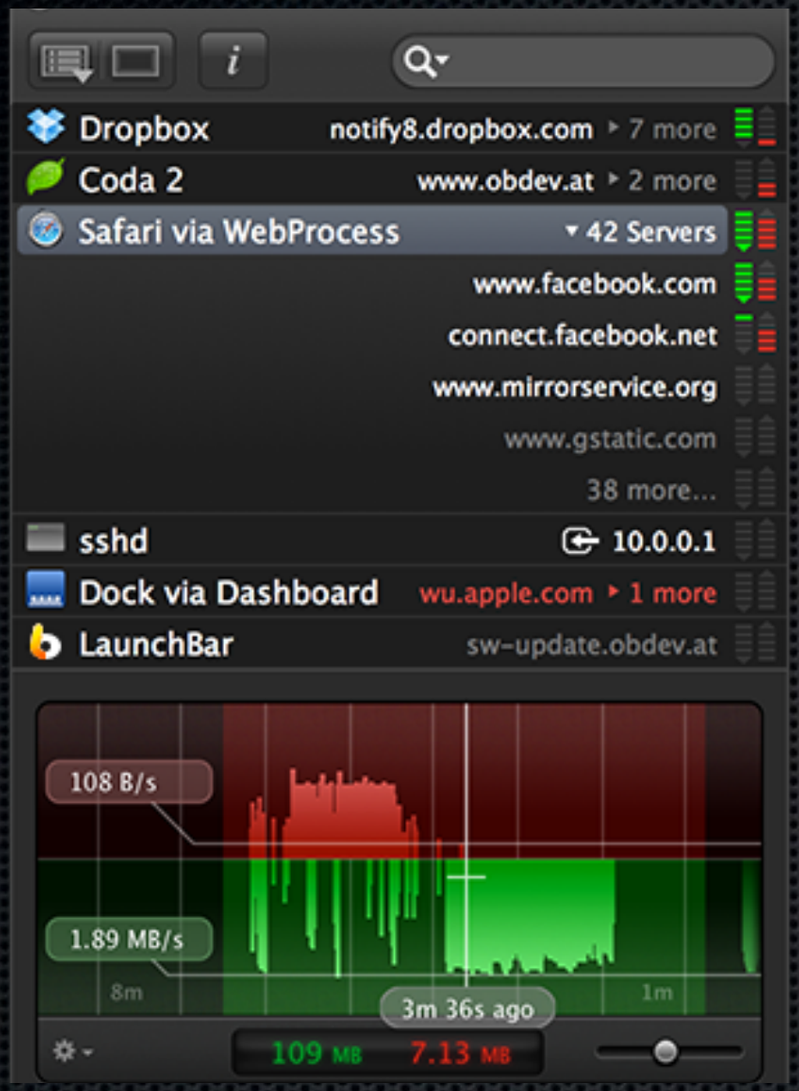
- With “appification", changes in user expectations
  - Free or very cheap apps
  - Software is throw away
  - Easy to obtain and try lots of software
  - Ad-supported
- New malware vector
  - The whole application is malware
  - Runs nefarious process as app runs
  - Ads need to keep network open for new ads and can share collected data about you
- Need to analyze software behavior

Backdoor.MAC.Eleanor

- Free App on MacUpdate "EasyDoc Converter"
- Unsigned
- Creates LaunchAgents that allow
  - filesystem access
  - remote code execution
  - webcam access



Little Snitch Network Monitor





- https://www.obdev.at/products/littlesnitch

Intrusion Prevention Systems

- Open Source intrusion prevention system capable of real-time traffic analysis and packet logging.
- Create rules based on detecting actual vulnerable activity.





Get Rid of These (if you can)









Microsoft® Silverlight™

iOS Security after a Decade

"No malware has affected iOS devices at scale."

Apple WWDC 2016



iOS Security Pillars

- iOS platform security
- Users consistently upgrading their software
- Developers building secure apps

iOS still has risks

- Vulnerabilities
- Exploits (e.g. Zerodium bounty)
- Malware (e.g. XcodeGhost)
- Social engineering
  - Phishing

iOS Precautions

- Configure complex passcode + TouchID



- Configure VPN
- Monitor iOS updates
- Push out app updates



OpenDNS

- Owned by Cisco
- Configure DNS service
- Provides protection from fraudulent web sites
- Can work on and off network



Mobile Device Management

- Distribute qualified software
- Inventorying to identify alien software
- Enforce security configurations
- Readily apply security updates
- Maintain known good states

End User Education is So Important

Who do you trust?

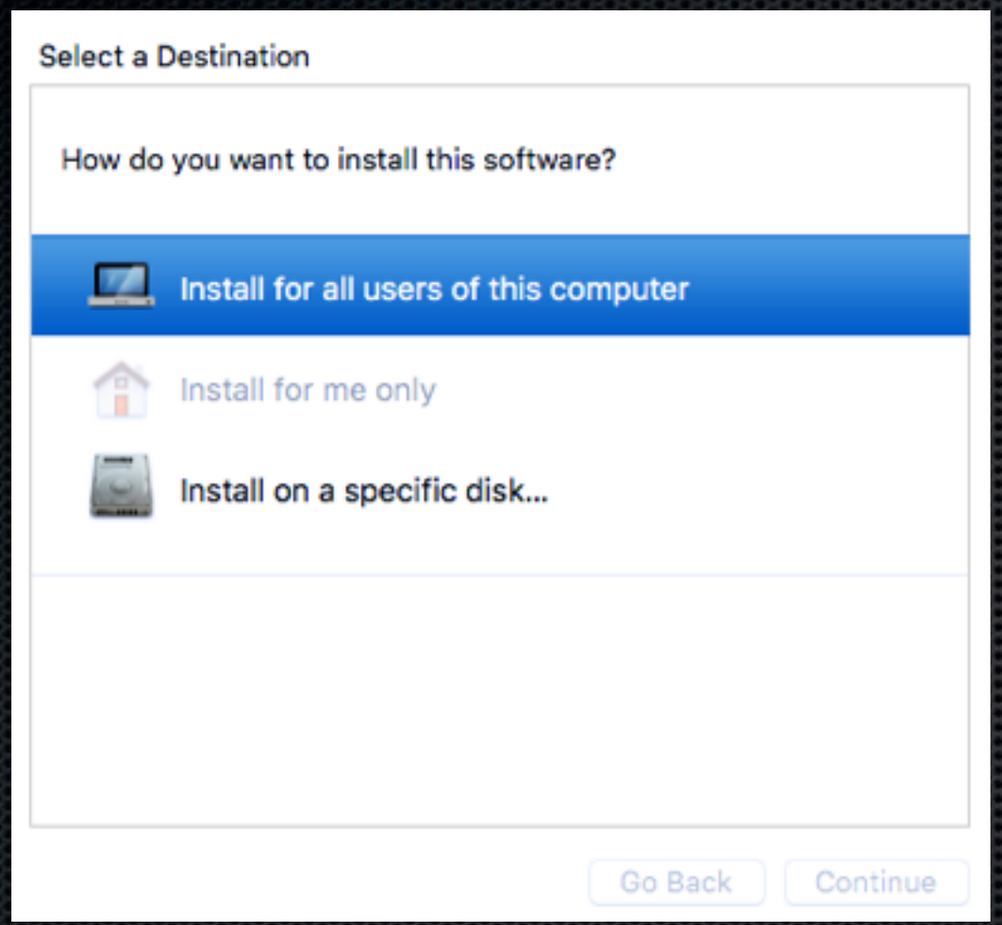
Before installing, you must truly understand:

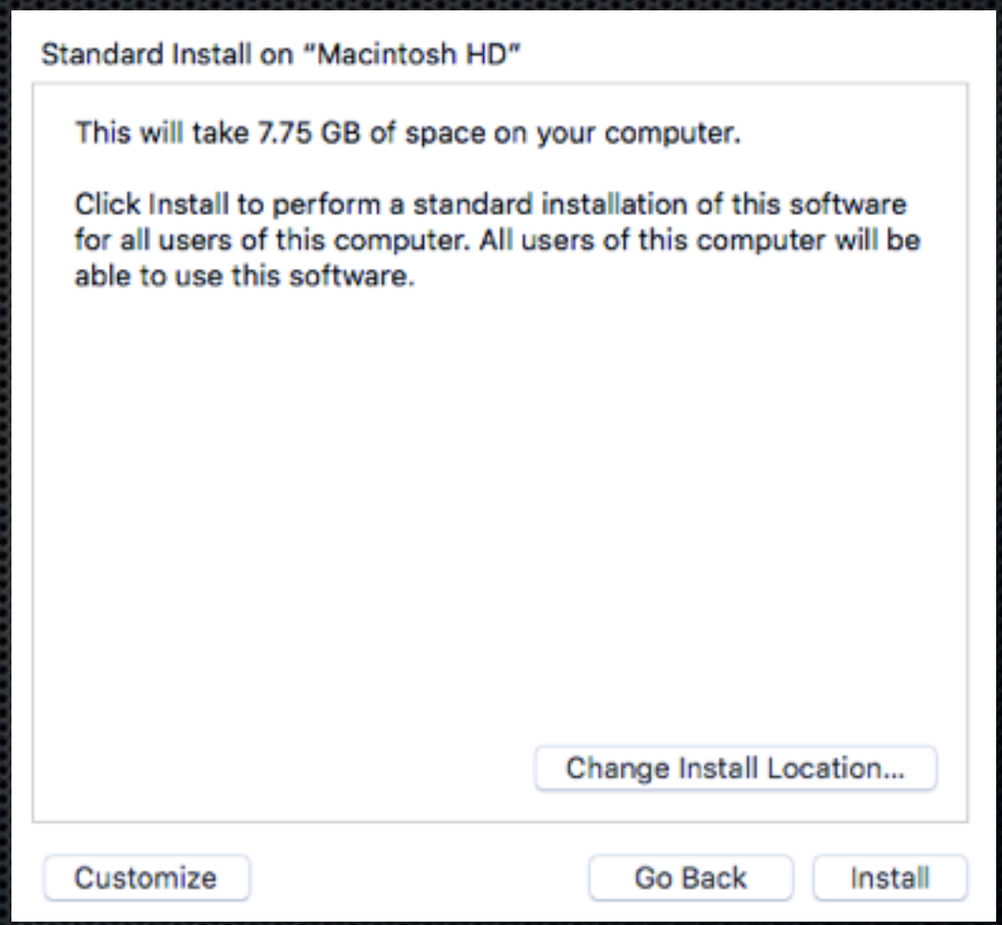
- the publisher of the software.
- the trust you are placing in the software.
- the quality of the on-line store or download site.
- your connection on-line via certificates.

Wants to Know Your Most Private Secret



Shared Filesystem Access





Perpetual Internet Connection



A Truly Secure System

- Prompt you for authorization each time:
  - the program is launched.
  - an Internet connection is made.
  - it access the filesystem outside its bundle.

End User Education is So Important

- Acknowledge that security is the opposite of convenience
- Be alert to unexpected or suspicious events
  - unexpected requests for password
  - prompts seeking approval to trust
  - being diverted to unfamiliar websites

Phishing

The process of trying to obtain confidential information by looking as if it is from a legitimate, trusted organization but contains a link to a fake server that replicates the real one.

Who Might be an Attacker?

- Criminals looking to hold your data ransom
- Business competitors looking for an edge
- Service providers tagging you for marketing
- Nation-states such as North Korea and Sony
- Romantic partners, family, friends out of curiosity

Software Management Models

- Fully locked down
- Hands-off
- Shared control

Resources

- Apple Security Updates: HT201222
- http://www.thesafemac.com
  - https://blog.malwarebytes.com/author/treed/
- https://www.av-test.org
- http://www.apple.com/osx/what-is/security/
- https://developer.apple.com/videos/play/wwdc2016/706/
- https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml#AppleMac

Questions?



Craig Doran
craig@machero.com

MACTECH PRO EVENTS