The State of Apple Security

Gary F. Alderson, Aldersoft

Presenter Introduction

- Gary F. Alderson
- Bachelor of Science (Computer Science), University of Manitoba
- CDP, Institute for the Certification of Computer Professionals (ICCP)
- Owner, Founder and CCBW of Aldersoft
- 40+ years experience in Information Technology
- 35 years at the University of Manitoba
- Chief Technical Architect of University of Manitoba System Renewal
- Manager, Integration Support, IST, University of Manitoba
- Retired: September 2010
- Email: Gary.Alderson@Aldersoft.CA
- Facebook: http://Facebook.com/aldersoft.ca

Apple's Security Model

- Apple is proprietary. Both Hardware and Software. IE. Apple controls its complete environment.
- Mac OS X is based on BSD Unix. (Berkeley Software Distribution).
- IOS is closed and proprietary.
- Apple strictly vets all software sold and distributed by the Apple Store.
- In essence, Apple is closed and isolated from the world and all of its evils and threats ... or is it ?

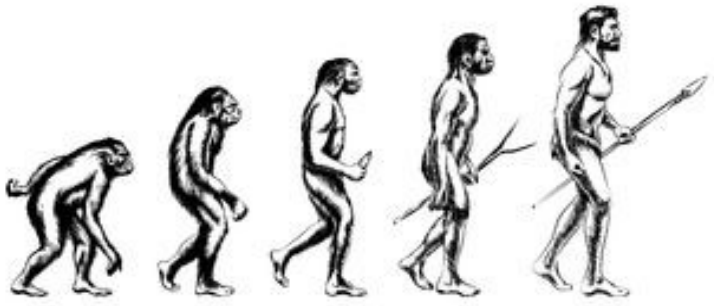
Trouble in Paradise ?

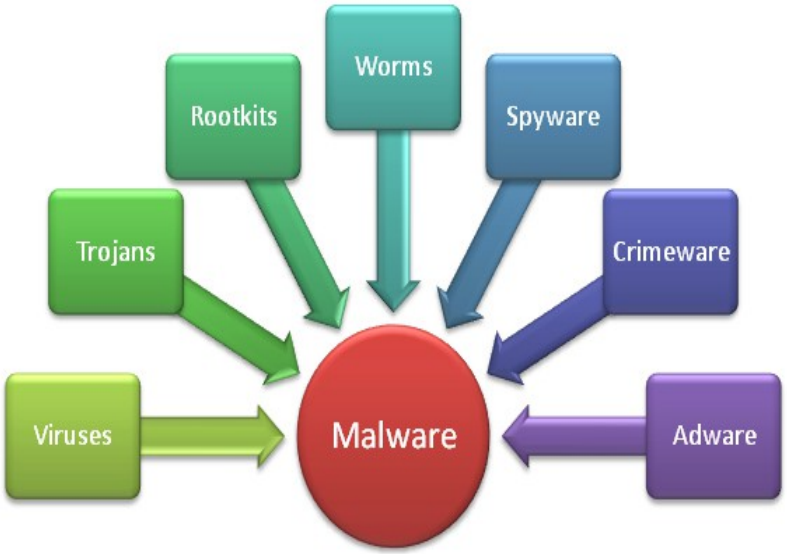
- Apple clients feel that their computers are safe. Hence many are complacent about security and safe computing practices.
- Apple employees, while very vigilent, are only human, thus subject to mistakes and unable to watch everything.
- Many IOS (iPhone, iPad, iPod) users hack their devices. Better known as “Jailbreaking” or “rooting” to perform restricted functions thus defeating security.
- Apple now uses several third parties and outside contractors to develop applications and toolkits.

Trouble in Paradise ?

- The bad guys are very mature and extremely dangerous these days. The Script Kiddies have become Cyber Terrorists and work for radical groups, governments and organized crime.
- Some governments have made cyberwarfare an integral part of their overall military strategy, with some having investing heavily in this capability.
- Cyber Terrorism is the new Atomic Bomb.

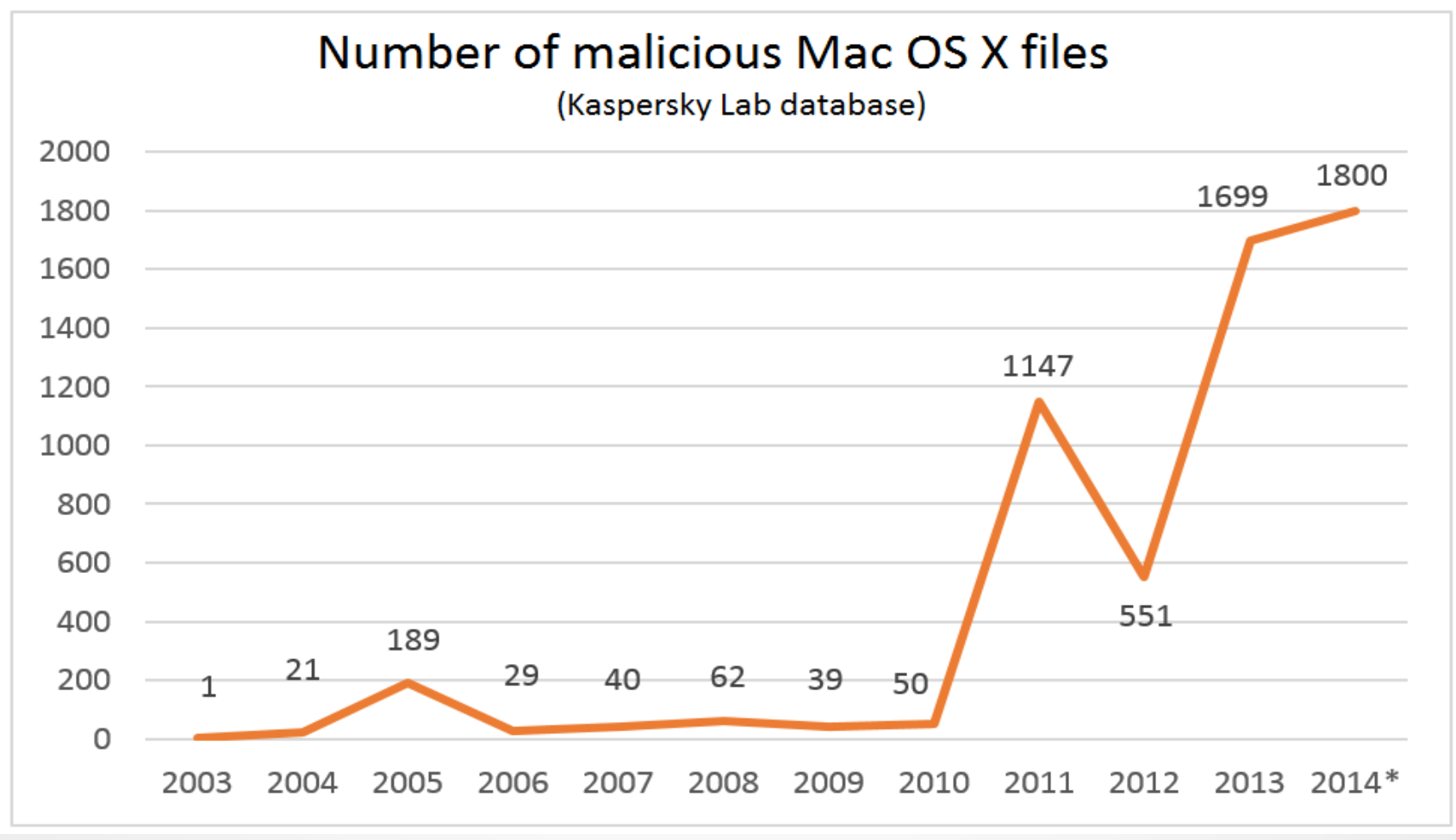
The Evolution of Malware



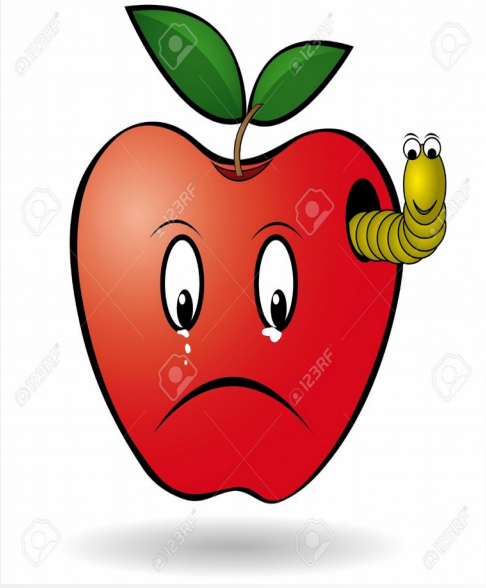


- 1949 - John von Neumann's article "Theory of self-reproducing automata" is published.
- 1971 - Virus – The Creeper. Self replicated across APRA Net. Testing John von Neumann's theory.
- 1981 - Elk Cloner, target Apple II systems. Responsible for the first large-scale computer virus outbreak in history.
- 1986 - The Brain boot sector virus released. Brain is considered the first IBM PC virus.
- 1992 - Michelangelo virus infected 5 million.
- 2005 - copy protection rootkit by Sony.
- 2013 - CryptoLocker Trojan horse. First Ransomware.
- 2015 - November - XCodeGhost Found Hiding In U.S. And In Apple iOS 9 Apps.
- (Source: Wikipedia: Timeline of computer viruses and worms)

So How is Apple Affected ?



Recent Apple Directed Attacks



- Youmi Ad SDK (October 2015)
- Muda (October 2015)
- YiSpecter (October 2015)
- XcodeGhost (September 2015)
- KeyRaider (August 2015)
- Lock Saver Free (July 2015)
- Xsser mRAT (December 2014)
- WireLurker and Masque Attack (November 2014)
- See list at Wikipedia: Malware for iOS

Siri's Lock Screen Bypass

- Reported November 18, 2015 by Trend Micro.
- “Security vendor Trend Micro has sounded the alarm once again on a continuing issue with Apple’s Siri digital assistant that lets anyone with physical access to an iOS device to interact with it and easily extract data even if the device is locked.”
- Solution: Disable Siri on the Lock Screen.

Ok. What should I do ?

- Backup your data regularly with a repudiable off-site storage vendor.
- Install AntiVirus Software.
- Install AntiMalware Software.
- Run/Schedule regular scans.
- No more Jailbreaking.
- Perform proper Security Hygene.
- Practice Safe Computing practices.
- Use commonsense.

Backup your data regularly

mozy BY EMC

Acronis

SugarSync

SpiderOak™

iCloud.com

BACKBLAZE

- In general, you should backup your data daily or weekly depending on how often it is changed.
- Use a repudiable backup company which has a proven track record.
- Backup data rather than synchronize it. This will maintain multiple versions over time, instead of just the latest copy.

Install Good AntiVirus Software

Avira

Bitdefender

eset

avast!

KASPERSKY lab

SOPHOS

- AntiVirus Software is still required.
- Some AntiVirus Software does not detect nor clean all MalWare.
- The leaders do both Viruses and Malware in a single product.
- See product reviews:
- TomsGuide.com Best Antivirus Software and Apps 2015
- TopTenReviews.com The Best Mac Antivirus Software of 2015

Install AntiMalware Software

Avira

VIPRE

AVG Anti-Virus

eset

Bitdefender

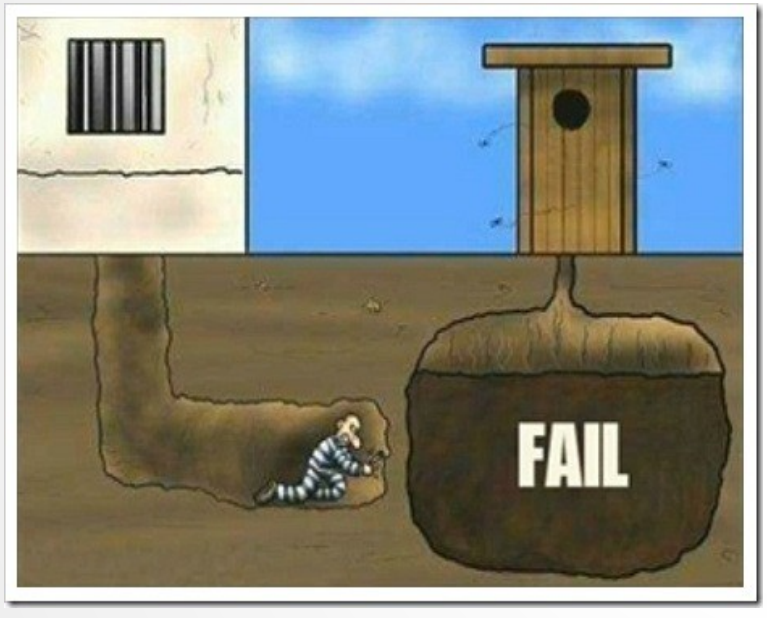
Malwarebytes

- What ? I just installed AntiVirus ?
- These days, you need a good AntiMalware product running too.
- Viruses are Malware
- Malware = Viruses + Trojans + Worms + AdWare + RansomWare + Rootkits + all other evils.
- Sometimes you need more than one to find really difficult MalWare

Run/Schedule regular scans

- Most AntiVirus and AntiMalware products will allow you to schedule regular scanning and disinfecting.
- Depending upon you usage, you should schedule these to run at least once a week.
- Always make sure that they are running in “Real Time” mode as well. This will prevent immediate threats.

No more Jailbreaking



- Jailbreaking can lead to very serious security problems.
- Unix systems need to strictly protect the “root” account. Even in experienced IT organizations, nobody logs in as root to ensure security.
- Apple provides the needed abilities such as Installing software, etc. indirectly.
- Use the “sudo” command if you absolutely must Jailbreak.

Perform proper Security Hygene

- Schedule and run regular backups !!!
- Regularly scan for Malware.
- Clear your Web Browser cache.
- Clear your cookies.
- Keep Software “reasonably” up to date and apply updates.
- Use good passwords and pins and change them at reasonable intervals.
- Don't write down your passwords or pins.
- Don't share your computer.
- Never ever share your passwords.

Practice Safe Computing practices

- Stay away from questionable websites.
- Be suspicious if you are asked for credit card information or any personal information.
- Use PayPal instead of credit cards for Internet payments. Link to cards with a low credit limit.
- Be aware of phone and email scams. And Never reply to the caller / sender.
- Only open email attachments from people that you know and even then be careful.

Use commonsense

- “If it seems to good to be true, then it probably is a scam.”
- Ask yourself “Why would Microsoft or CRA (Customs and Revenue) call me at home ?”
- Tell callers to phone back at a specific day and time. Chances are they won't bother.
- Play dumb. “But I don't own a computer. How could it have a problem ?”

Questions and Answers ?