

Cyberdefence Seminar

Ahto Buldas



Mac OS X and iOS security

Heliand Dema

Desktop and mobile OS share

Mobile Market Share (including Tablets)

✓ Mobile/Tablet Browser Share





 Safari	62.0%
 Android Browser	18.6%
 Opera Mini	13.1%
 Symbian Browser	2.6%

✓ Mobile/Tablet O/S Share

 iOS (iPhone, iPad, iPod)	61.5%
 Android	18.9%
 Java ME	12.8%
 Symbian	3.5%

Desktop Market Share

✓ Desktop Browser Share

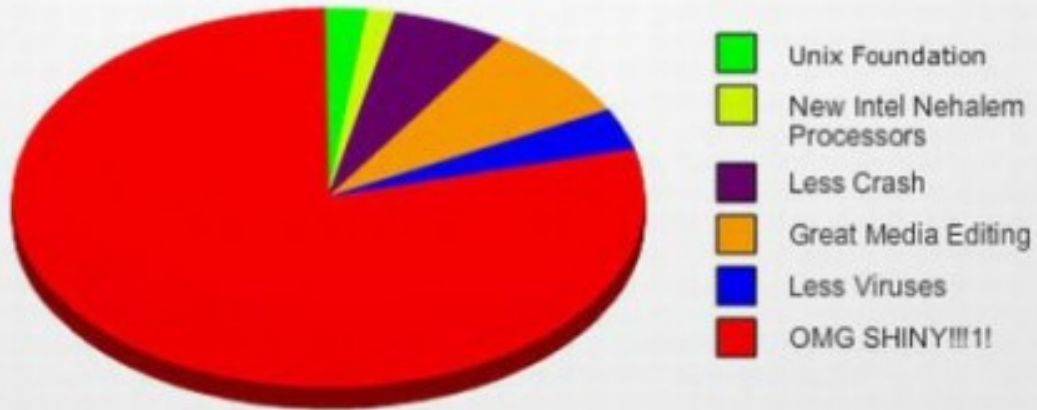
 Internet Explorer	52.6%
 Firefox	22.5%
 Chrome	17.6%
 Safari	5.4%

✓ Desktop Operating System Share

 Windows	91.9%
 Mac	6.9%
 Linux	1.2%
 SunOS	0.0%

Why mac?

Reasons People Want A Mac



What does Apple say?



It's designed to be a better computer.



It comes with software you'll love to use.



It comes with the world's most advanced OS.



It comes with award-winning support.



It runs Office and works with your existing PC files.



It's compatible with your stuff.



It doesn't get PC viruses.



It's loaded with the latest technology.

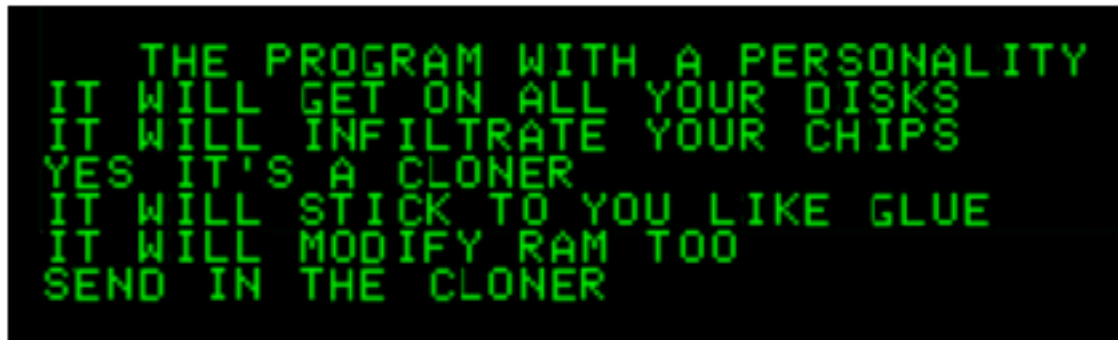


It runs Windows and Windows applications.

History of Mac malware :

Apple Computer Inc. was given the historic honor of being the first computer to bring virus technology into the home.

✧ **1982** - 15-year-old student Rich Skrenta wrote the Elk Cloner virus, capable of infecting the boot sector of Apple II computers.



```
THE PROGRAM WITH A PERSONALITY  
IT WILL GET ON ALL YOUR DISKS  
IT WILL INFILTRATE YOUR CHIPS  
YES IT'S A CLONER  
IT WILL STICK TO YOU LIKE GLUE  
IT WILL MODIFY RAM TOO  
SEND IN THE CLONER
```

✧ **1987** - The nVIR virus began to infect Apple Macintosh computers, spreading mainly by floppy disk. Source code was later made available, causing a rash of variants for the Mac platform - The first anti-virus products for Mac.

✧ **1988** - Running on early versions of Apple's Mac OS, one HyperCard virus displayed a message about Michael Dukakis's US presidential bid before self-destructing:

✧ **1990** - The MDEF virus infected applications and system files on the Mac.

✧ **1991** - HC (also known as Two Tunes or Three Tunes) was a HyperCard virus discovered in Holland and Belgium. On German language versions it would play German folk tunes and display messages such as "Hey, what are you doing?"

History of Mac malware :

- ✧ **1995** - Microsoft accidentally shipped the first ever Word macro virus, Concept, on CD ROM. It infected both Macs and PCs running Microsoft Word. Easy to create variations - kids found a new way to kill their free time.
- ✧ **1996** - Laroux, the first Excel macro virus, was released and hit owners of Windows computers. Mac users escaped unaffected at first - at least until the release of Excel 98 for Mac.
- ✧ **1998** - AutoStart 9805 worm - spread rapidly in the desktop publishing community via removable media, using the CD-ROM AutoPlay feature of QuickTime 2.5+. (Asia)
Sevendust, also known as 666, infected applications on Apple Mac computers.

Mac OS v10.0 "Cheetah" - a whole new version of the operating system - the old malware would no longer be capable of running.

- ✧ **2004** - The Renepo script worm (aka "Opener") attempted to disable Mac OS X security including the Mac OS X firewall.
In addition, the Renepo worm would download and install hacker tools for password-sniffing and cracking, make key system directories world-writeable, and create an admin-level user for hackers to later abuse.



History of Mac malware :

✧ **2006** - OSX/Leap-A was programmed to use the iChat instant messaging system to spread itself to other users. Was deleting files from system. First virus or worm for OS X!?

-Macarena

✧ **2007** – The first financial malware for Mac was discovered. The gang behind the attacks developed both Windows and Mac versions of their OSX/RSPlug-A Trojan horse. The Trojan posed as a codec to help users view pornographic videos, but in fact changes DNS server entries.

✧ **2008** - Poisoned adverts on TV-related websites. If accessed via an Apple Mac, surfers would be attacked by a piece of Macintosh scareware called MacSweeper or Imunizator.

OSX/Hovdy-A Trojan horse was discovered that could steal passwords from Mac OS X users, open the firewall to give access to hackers, and disable security settings.

Troj/RKOSX-A was discovered - a Mac OS X tool to assist hackers create backdoor Trojans, which can give them access and control over your Apple Mac computer.

Apple issued a support advisory urging customers to run anti-virus software – but after media interest, rapidly deleted the page from their website.

Fully patched MacBook Air was hacked by **Charlie Miller** in 2 minutes!!! 😊

History of Mac malware :

✧ **2009** - OSX/iWorkS-A Trojan horse distributed via BitTorrent inside pirated versions of Apple's iWork '09 software suite Adobe Photoshop CS4.

- *RSPlug Trojan* horse appeared on websites, posing as an HDTV program called MacCinema.

Apple finally began to introduce some anti-malware protection into Mac OS X.
Charlie Miller says hello...again!!!

✧ **2010** - OSX/Pinhead Trojan (aka HellRTS).

- *Boonana* cross-platform java worm
- *Spynion* (aka OpinionSpy)

✧ **2011** - BlackHole RAT, a Trojan allowing hackers to gain remote access to your Mac. Inside the code:

*"I am a Trojan Horse, so i have infected your Mac Computer. I know, most people think Macs can't be infected, but look, you ARE Infected!
I have full controll over your Computer and i can do everything I want, and you can do nothing to prevent it.
So, Im a very new Virus, under Development, so there will be much more functions when im finished."*

History of Mac malware :

2011 - Mac Defender (aka Mac Protector, Mac Security, Mac Guard, and Mac Shield)

Apple's support reps were ordered not to help users remove the malware.

The Mac security firm Intego discovered the fake antivirus software on May 2, 2011, with a patch not being provided by Apple until May 31!

- "Do the Diaoyu Islands belong to Japan?" . OSX/Revir-B Trojan appeared to disguise itself as a PDF file about a controversy between Japan and China about the Islands.

- Flashback Trojan horse disguised itself as an update for Adobe Flash. OSX/FlashPlyr-A could allow a remote hacker to gain access to your computer or download further malicious code to your Mac.

- Could a remote hacker do something to cause physical damage to a computer?
C.M. - Spyware onto your battery chip - default password for battery's firmware

Resolution: Referred Customer; to either Apple Web Site or third party as appropriate.

Things you must never do according to the client:

-You cannot show the customer how to force quit Safari on a Mac Defender call.

-You cannot show the customer how to remove from the Login Items.

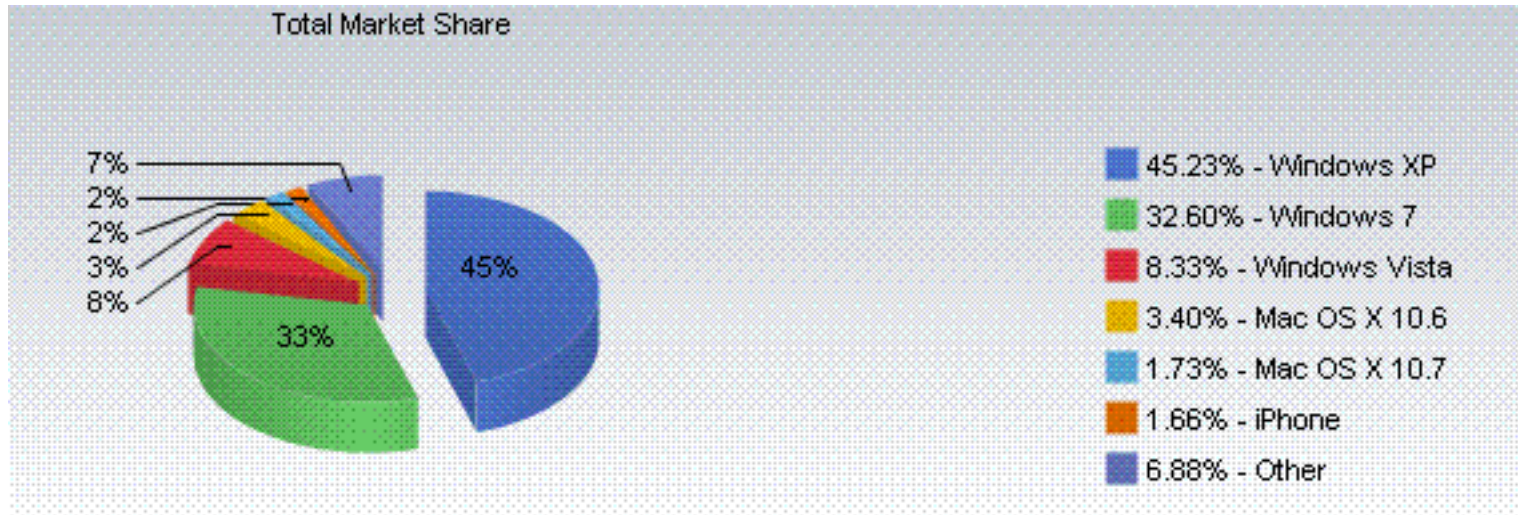
-You cannot show the customer how to stop the process of Mac Defender in their Activity Monitor.

-You cannot refer the customer to ANY forums or discussions boards for resolution (this includes the Apple.com forums)

Something cool:



Mac OS X Security issues:



1. Firewall off by default – no notification
System Preferences-Security and Privacy-Firewall
20% know what a firewall is, only 5% will turn it on
80% think their mac is beautiful
 - Snow Leopard uses same ASLR as Leopard

Mac OS X Security issues:



Applications on the Mac OS X system are structured using an architecture called a "bundle". A bundle is a special folder that pretends to be a single file.

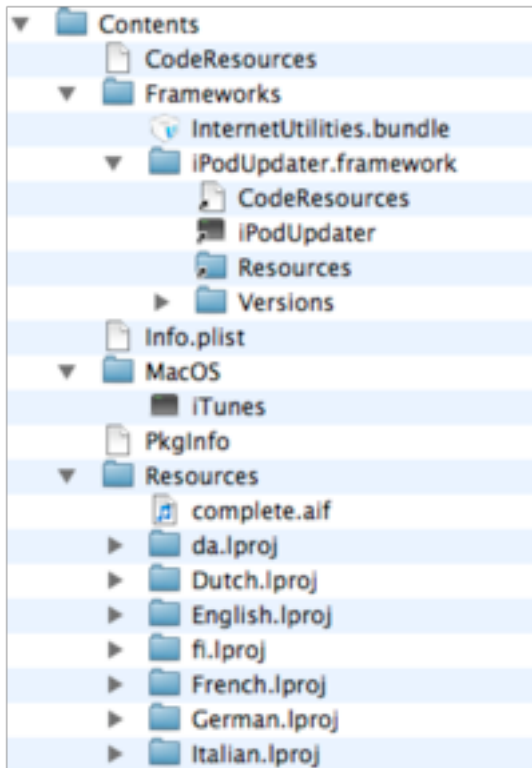
The advantage of this, for programmers, is that it allows multiple resources to be contained in one single folder.

Apple also use the bundle format for many of their pro tools to save documents.

The structure of the bundle architecture makes it easier to insert executable code within an existing trusted application by simply renaming the existing executable e.g. iTunes found in the MacOS subfolder and inserting a second executable into the MacOS folder with the original's executable name.

When the user executes the bundle (in this case iTunes.app) the virus code would execute instead.

The virus would then launch the renamed iTunes executable so that the user would not be aware they had run the wrong program.



Mac OS X Security issues:



Programs that a user relies upon and considers part of their system such as iTunes, iChat, Keynote, etc. are stored unprotected inside a folder called “/Applications”. Any program running on a Mac OS X system can write to this folder and to most of the contents.



A Mac OS X Address Book.

This database keeps track of all other contacts the user communicates with including their instant messaging addresses, email addresses, phone numbers, physical addresses, etc. **The database is open to access from all programs running on the Mac OS X computer.**

Remember the “ILOVEYOU” worm?

Mac OS X Security issues:



Apple's anti-malware protection only protects you against a handful of Mac malware, doesn't defend you if you try to copy an infected file from a USB stick for instance, and doesn't offer clean-up facilities.

Flashback Trojan horse

Users that keep their Safari system settings standard are at the greatest risk because the Safari browser is set to consider installer packages as safe (those files with a .pkg or .mpky extension) it will automatically launch after download.

Apple - OS X Lion - The world's most advanced OS.

- ✓ Firewall still off
- ✓ Attacks via Firewire / IEEE 1394

What can someone do?

- ❖ read arbitrary RAM contents from the victim's system,
- ❖ overwrite arbitrary RAM contents with whatever you want,
- ❖ perform many, many severe attacks based on the two issues above.

Examples include grabbing a full RAM dump via Firewire (takes only a few minutes), grabbing ssh-agent keys, grabbing screen contents, modifying screen contents, bypassing login/password screens, and many, many more...

- ✓ Mac OS 10.7 has two major flaws in the OS's Directory Services:
 - the ability for non-root users to view password hash data
 - the fact that passwords can be changed by anyone

```
$ dscl localhost -passwd /Search/Users/Heliand
```

iOS Security

Apple's iOS operating system powers iPod, iPhone, iPad and 2nd Gen Apple TV is a Unix-based system.

200 different vulnerabilities in various versions of the iOS.

Most allow attackers access to single process (e.g. Safari process).

Majority of exploitation have been initiated by device owners for jail-breaking.

Total iPhones Sold Worldwide - 108 million

Total iPhones Jailbroken - 30 million

- Login: root - alpine

Apple took an average of 12 days to patch each vulnerability once it was discovered

iOS Security issues:

Over 200 vulnerabilities since 2007

iPhoneOS.Ikee Worm - This worm spread over-the-air to jailbroken iOS devices, changing the device's background wallpaper

iPhoneOS.Ikee.B - Spread over-the-air to jailbroken iOS devices. Once the worm infected a new device, it would lock the screen and display:

*"Your iPhone's been hacked because it's really insecure!
Please visit doiop.com/iHacked and secure your iPhone right now!"*

Jailbreakme.com – 2 exploits in 1.

PDF -The way Safari parses PDF files, enabling the code to get inside a protective sandbox.
MobileSafari - Allows code to break out of the sandbox and get root

Average jailbreaking time:

10 sec if user under 60 years old

35 sec if user older (or doesn't know how to type)

P.S. Apple is hiring hackers ;)

Is iOS secure?

- iOS's encryption system provides strong protection of emails and email attachments, and enables device wipe.
- iOS's isolation model totally prevents traditional types of computer viruses and worms.
- iOS's permission model ensures that apps can't obtain the device's location, send SMS messages, or initiate phone calls without the owner's permission.
- The OS protection methods Apple uses (ASLR - Address Space Layout Randomization and DEP - Data Execution Prevention) makes iOS more secure.
(Android does not use these protection methods)
- ~~Apple vets every single publicly available app which has by far proved a good protection against malware attacks, data loss attacks, data integrity attacks.~~

InstaStock, stock checking app by Miller, was approved to app store. The app let him download photos, a contacts database and even vibrate the phone.

Are iOS apps secure ?

All bets are off when an Apple device is jailbroken!!

Conclusion:



What must Apple do:

- Kill Charlie Miller
- Firewall notification
- Ask for password when moving files to Application folder and when editing apps
- Try to release patches asap

What must users do:

- Save Charlie Miller's life
- Check firewall and its rules (Stealth – on). Review default options on your apps.
- Install Anti Viruses (Sophos) and Networking Monitoring Apps (Little Snitch)

On iOS

- Change the default SSH (root) password.
- SSH – Turn it off (Install SBSettings from Cydia) – WiFi - off
- Read before you download!

Questions:

MacBook first to fall @ Pwn2Own 2011



THNX