

Robert Hammen

Robert Hammen, Senior Systems Engineer, MC Services, <http://www.mcservices.com>

I have been supporting Macs since before the first time Apple was doomed. I hold all of Apple's IT certifications going back to OS X 10.4. I am also an Apple Certified Trainer (Support Essentials and Server Essentials). I have many years of JAMF Casper Suite administration and management experience.

MC Services is a Wisconsin-based Apple-centric consulting and training firm (with a new Lake Bluff training center opening soon!). I perform work for clients large and small, as well as teach training classes.



Security, Viruses, Adware
and Malware, Oh My!
It's real. It's now.
You need to take it seriously.

What's the difference?

- Viruses
- Malware
- Trojan Horses
- Adware
- Fakeware

Viruses - a very brief history

- 1980's forward, Mac was an uninfected carrier
- “Typhoid Mac”
- nVIR (Classic Mac OS)
- Word Macro Viruses in mid-90's

Malware

- Initially in pirated downloads
- Also encompasses keyloggers and “backdoors”
- Primarily on Windows PC’s - botnet
- Also on Windows PC’s - cryptolocker
- \$\$\$

Trojan Horse

- Something that is not what it appears
- 2012 - Flashback for Mac
- Fake Flash, MPlayer, video codecs

Adware

- Geneio Search
- vSearch
- Conduit
- Redirected search results, pop-ups
- \$\$\$

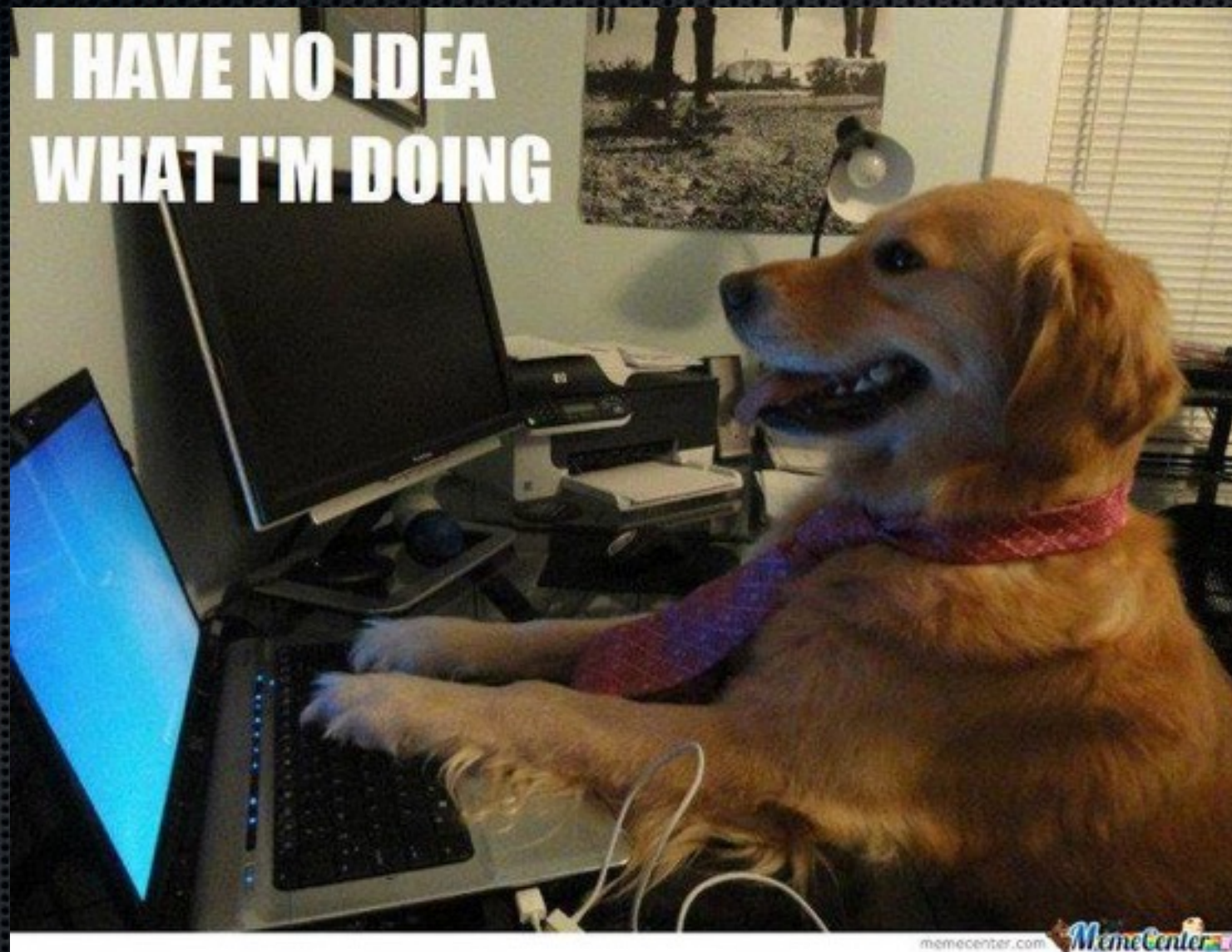
Fakeware

- MacDefender (no longer a concern)
- MacKeeper
- MacProtector
- various Mac “cleaning” tools
- \$\$\$

Security Implications

- Pop-ups and search redirection
- keyloggers - compromise passwords and credit cards
- Remote Control - privacy
- Compliance issues - PCI, SOX, HIPAA

How are systems affected/ infected?



How are systems affected/ infected?

How Computers Get Infected

Computer infections for home users are defined by malicious or unsavory programs being able to run on your computer and do what you can do - or more.

If you can see something, they can see something.

If you type something, they can read what you type.

If you can talk to the Internet, they can talk to the Internet.

If you can edit a setting, they can edit a setting.

That's a lot of power. How does this happen?

You get tricked

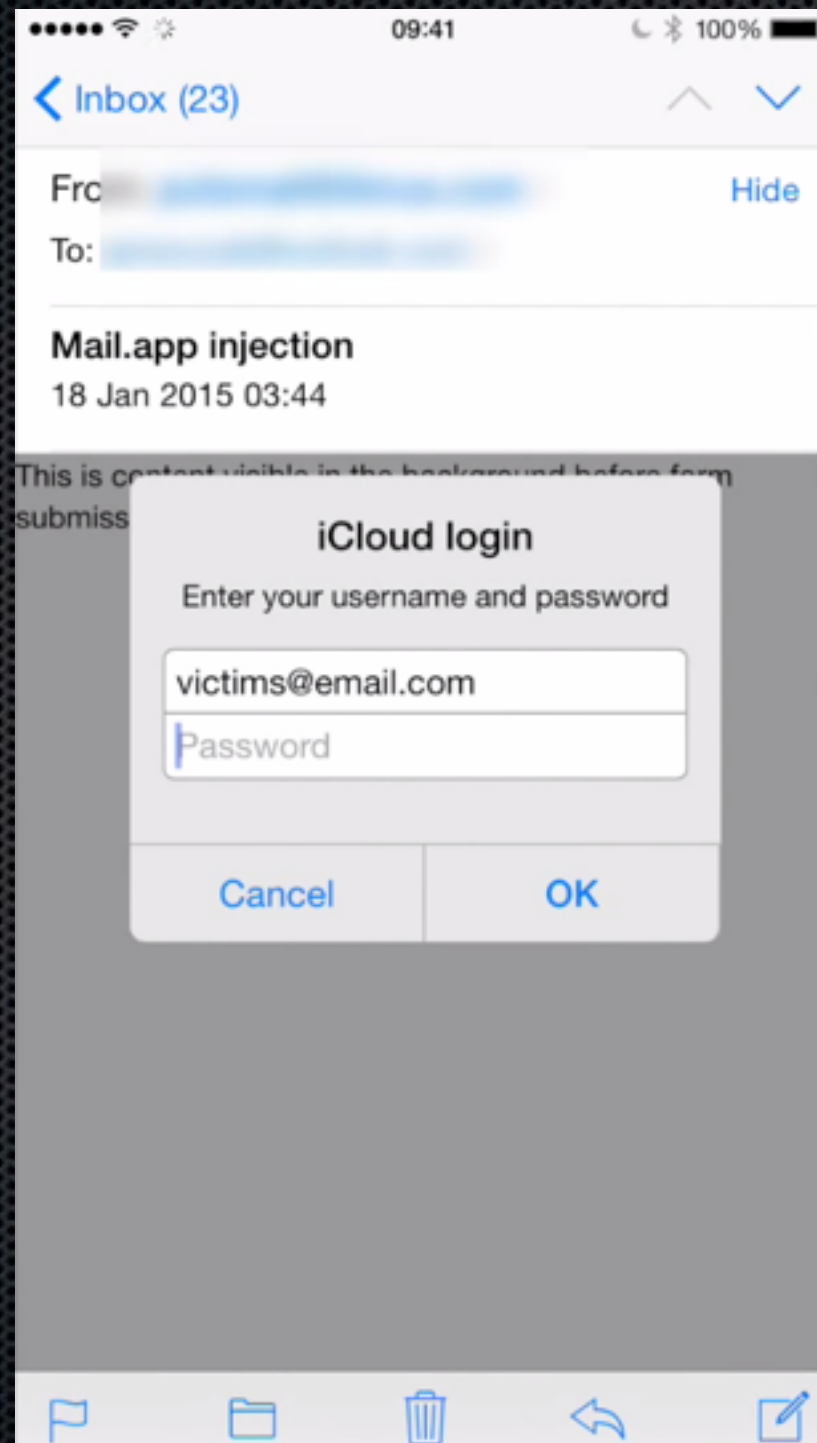
"But I'm too smart to get tricked."

- You

How are systems affected/ infected?

- Email attachments
- Password prompts
 - Users trained to just blindly enter passwords
 - Can be spoofed/faked

How are systems affected/ infected?



How are systems affected/ infected?

- Downloading Software
 - Poor Internet Hygiene - Googling
 - Sites like download.com, softonic.com
 - Even good sites go bad - sourceforge.net
 - VLC and MPlayer
 - Flash Player

Security vs Usability

- The classic tradeoff
- Too much security - makes system unusable
- Too little security - makes system vulnerable

How to Stop?



How to Stop?



SECURITY CHECK 

Is there your card in the hackers database?
You can easily check here, just enter your card info:

Card number:

CVC@ (CW2):

- Education
 - Where to get software - vendor or MacUpdate
 - What software to get
 - When to enter your password
 - Careful with email attachments

Admin vs non-Admin users

- Are your users Admins?
- If so, why?
 - Authorization
 - Secondary Account w/admin credentials

Firewalls

- Network
 - Many vendors have higher-end firewalls with anti-malware and intrusion detection abilities
 - Cisco, Sonicwall, etc.
 - Not inexpensive, typically yearly fee

Mail Servers

- If you host/manage your own, be sure it's locked down
- Use SSL for IMAP, SMTP, and webmail
- Use Real-Time Blacklists, SpamAssassin, attachment filters, and maybe an anti-spam service or appliance (Barracuda)

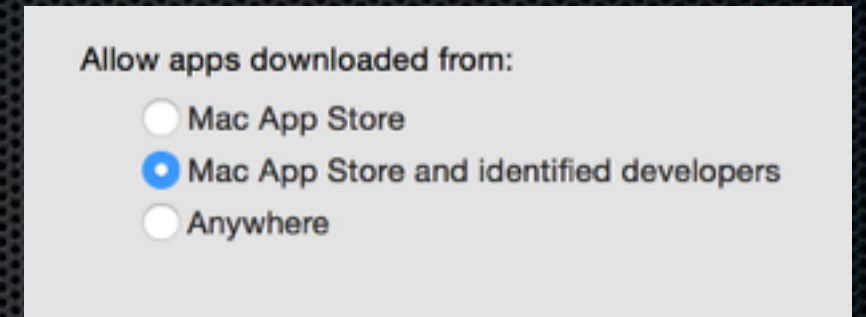
VPN

- Encrypts network traffic
- Critical for Offsite Workers and Remote Access
- Public WiFi + unencrypted passwords = bad
- Don't expose services to Public Internet
- Can be router/appliance or OS X Server

Secure Sockets Layer

- Encrypt Everything Everywhere
- Use for email (IMAP, SMTP)
- Use for calendars (CalDAV)
- Use for contacts (CardDAV, LDAP)
- Use for websites (https)

Gatekeeper




- Restricts what apps can be opened
- Restricts what software can be installed
- Default behavior is Mac App Store and Registered Developers
- Admin users can temporarily bypass
- Do not change default behavior unless you have a very good reason

XProtect

- Built-in anti-malware on OS X (since 10.6)
- Apple maintains a list of “bad” programs/processes/plugins - prevents them from running
- As of 10.9, useless if your Mac doesn’t check for software updates
 - softwareupdate - - schedule on
 - softwareupdate - - background-critical

XProtect



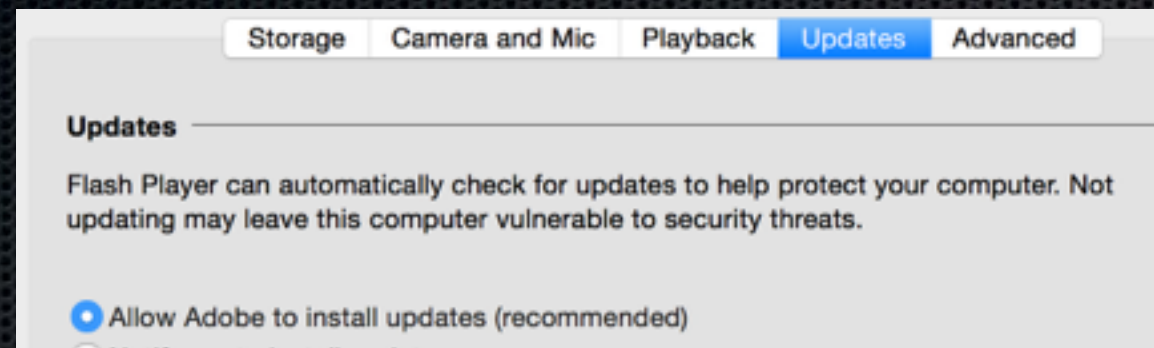
Software Update

ON

Settings Updates

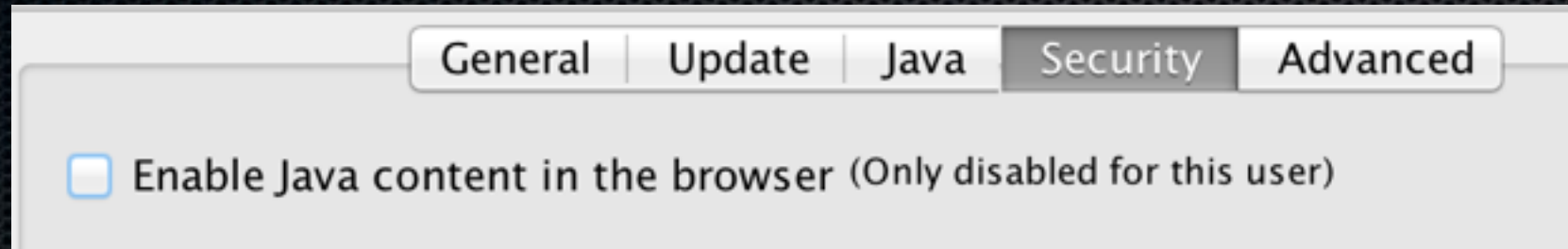
Name	Version	Date	Size	Status
XProtectPlistConfigData	1.0	07/15/15	11.57 KB	Enabled
Mac mini EFI Firmware Update	1.8	07/15/15	4.45 MB	Enabled
OS X Update Combined	10.10.4	07/14/15	2.07 GB	Enabled
OS X Update	10.10.4	07/14/15	1.87 GB	Enabled
Chinese Word List Update	3.19	07/14/15	113.98 KB	Enabled
iTunes	12.2.1	07/13/15	226.44 MB	Enabled
AppleConnect	2.8.1	07/09/15	18.33 MB	Enabled
Digital Camera RAW Compatibility Update	6.05	07/09/15	7.5 MB	Enabled
Gatekeeper Configuration Data	73	07/06/15	3.47 MB	Enabled

Flash Player



- Multiple Updates Per Month for exploits
- Do you really need it?
 - Google Chrome - integrated PepperFlash player
 - ClickToFlash + Allow Adobe to install updates

Java



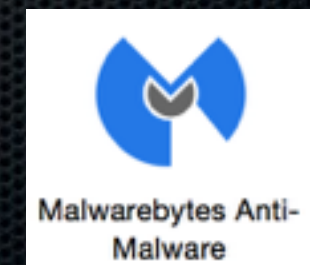
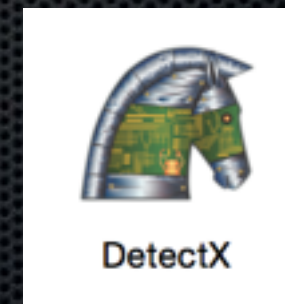
- Do you really need it?
- Do you really need it in a browser?

Antivirus

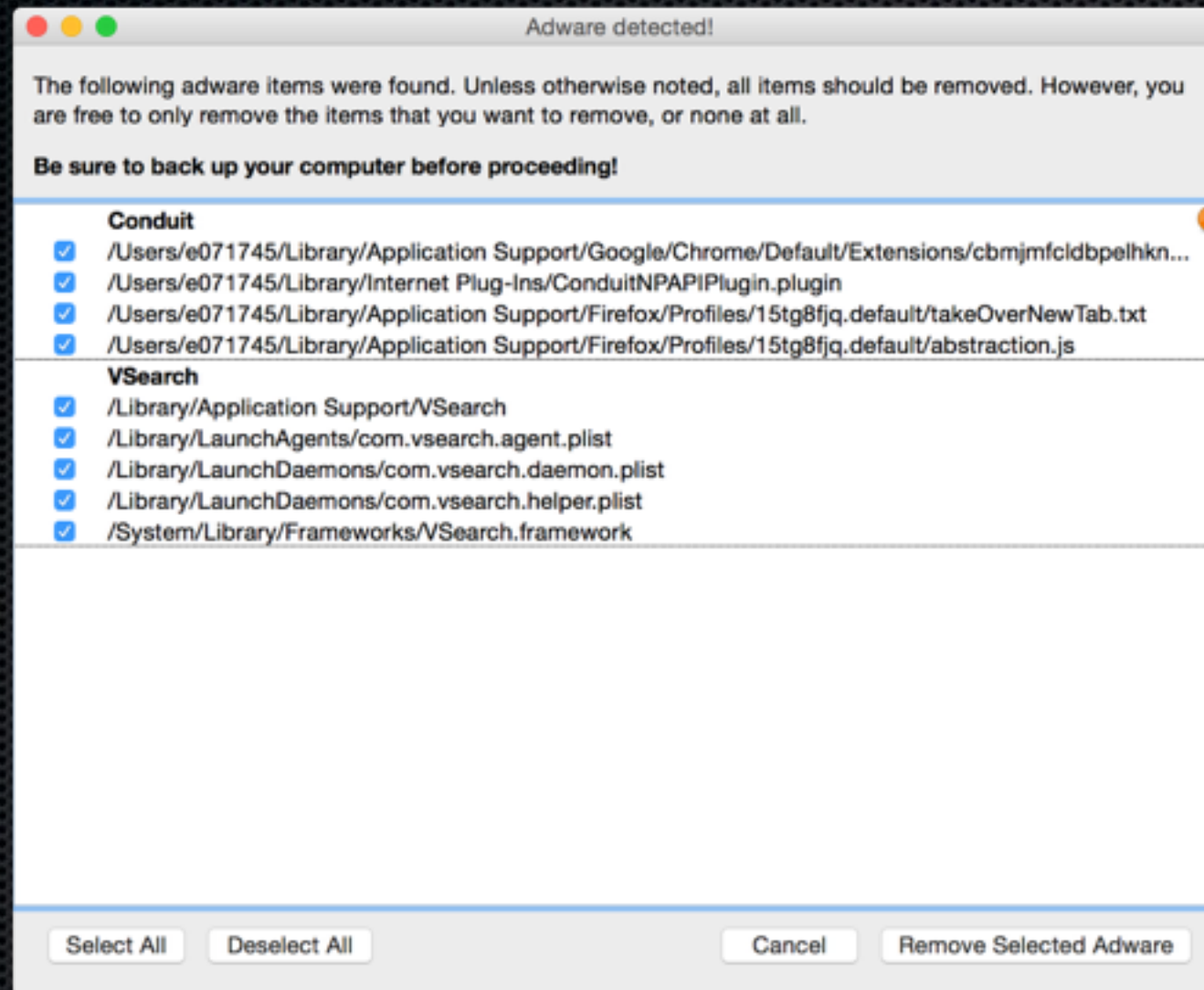
- May stop the bad guys
- Can have a terrible effect on performance
 - On-Access Scanning in particular
- Personal Experience with McAfee, Symantec, and Sophos
 - Sophos seems to have the least undesired side effects
 - For enterprise, need a Windows console
 - Installers are no longer standard packages

Antimalware

- Some of the Antivirus programs will stop
- XProtect
- DetectX - another arrow in the quiver
- AdwareMedic was free, but acquired by MalwareBytes last week (free for now)
 - Expect an Enterprise version (\$\$\$)



Antimalware



Other Tools

- Management software such as Watchman Monitoring detects malware and notifies you
- Casper Suite
 - Extension Attribute
 - Smart Group
 - Policies to remove

Backups

- Important if a system is
 - Too mission critical to take a chance
 - Too far compromised to be repaired
- Data should exist in AT LEAST 2-3 places
 - One of them should be offsite (fire/theft/disaster)

Passwords

- If a service supports two-factor, use it!
 - AppleID, Google, Facebook, Twitter, et. al.
- Don't make them simple words or names
 - Length is important
- Phrases not Passwords
 - <http://xkcd.com/936>
- Use a Password Manager
 - iCloud Keychain, 1Password, etc.

Passwords

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor&3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A SLOKEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

iOS

- Estimated over 5% of iPhone users (globally) have jailbroken their devices
 - ssh enabled w/default password - bad news
- Even non-jailbroken phones could be susceptible
 - stay on top of iOS versions
- Complex Passcodes, Activation Lock, Find My iPhone, Remote Wipe
 - MDM service like Bushel, AirWatch, Casper

More Resources

- <https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/>
- <http://www.thesafemac.com/mmg-catalog>
- <http://jamfnation.jamfsoftware.com>
- <http://derflounder.wordpress.com>

Questions?



Robert Hammen

robert@mcservices.com

Twitter: @hammen