Darrell Miller

Digital Forensic Examiner and System Administrator for Louisiana Attorney General's Cyber Crime Unit (CCU). ENCE Certified, Expert witness on digital forensics and data recovery at state and federal level.

The CCU assist all law enforcement in the state of Louisiana with cases involving technology. (local, state, federal agencies) Provide training and technical assistance in gathering evidence off all digital devices. Proactive and Reactive investigations.

~3500 to 4000 tips & calls a month on cases in Louisiana alone.
23 full time employees
~125 affiliate agencies
Maintain ~ 50 apple computers, 30 PC's, 2 apple servers & almost a petabyte of case data.



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

MACTECH PRO EVENTS

Perfect Security

- Security is a trade off between convenience and safety
- You have to work with your clients/users to determine what level of security you and they are comfortable with.
- You have to be willing to say "no", sometimes.

Layers of Security (Simplified)

- 1st layer - Firewall & Network Security
- 2nd Layer - System/Physical Security and User Policies.

Developing a strategy

- Define the needs
  - Larger Deployment
  - Small groups
  - Individual users
- Identify the best software for your specific environment
- Determine your strategy (ex: Server Malware scanning v. Desktop)
- Provide training/user education for the system you deploy

Viruses, the history of viruses coming to our platform

- 1980's forward, Being an uninfected carrier
- 1990's forward, Word Macro Viruses
- AdWare: First appeared in 2012
- Trojan horses appeared on Mac in 2012 (Flashback Trojan)

What's the difference?

- Viruses
- MalWare
- AdWare
- Trojans
- Windows Viruses

Moving from complacent to vigilant one decade at a time

- Virus scanning software an Enterprise requirement
- Virus scanning software a best practice
- Virus scanning software, it may be necessary to protect productivity

Statistics

- Estimated over 5% of iPhone users (globally) have jailbroken their devices. (KeyRaider: ~250k apple ids stolen)
- Even non-jailbroken phones could be susceptible
- Millions of Macs are likely infected and people don't know (e.g., emails with Windows viruses).
- Likely a large portion of those Macs are infected and causing trouble

Email Continuity, Spam and Virus filtering

- MXlogic
- SpamSoap (now Nuvotera)
- eVitera
- Barracuda's ESS
- Network appliances

Monitoring your Network and Systems

- Watchman Monitoring:
  - software, hardware, backup systems, drives, raid, network performance, system performance, malware, demographics/ hardware inventory info
- What are you monitoring?
  - bandwidth?
  - server activity?
  - database activity?
  - web traffic?
  - users themselves?
  - hardware health?
- Activity Monitor.. Solarwinds, Spiceworks

Avoiding Adware Scanner Utilities

- How bad is Genieo?
  - Genieo virus
  - Hard to remove. Proceed with caution
  - Utilities for removal
    - * Ars Technica article today
- MacProtector
- MacKeeper
- Avoid good software from bad sources.

Tools to use

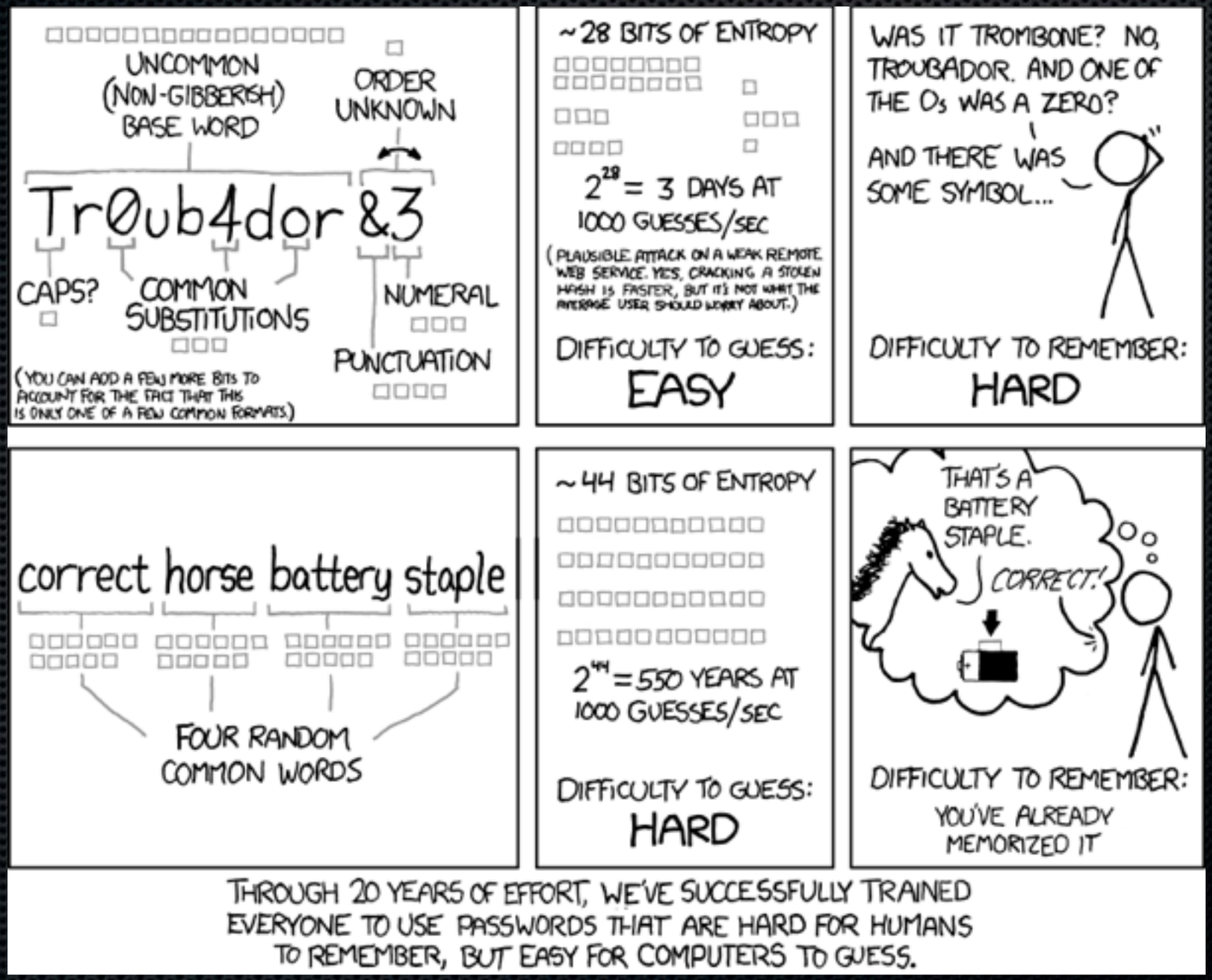
- BitDefender Virus Scanner: Free
- Sophos
- Kaspersky
- McAfee & Symantec
- Watchman Monitoring alerts
- AdwareMedic/Malware-bytes
- Virtual Machines (vmware, parallels, virtual box)

Password management

- Myths
  - Changing passwords every xxx days is a myth, and causes other problems
  - Myth: You shouldn't use real words. Truth: You can if long enough
  - Myth: Don't write things in Apple Notes, OneNote or other note taking software.
- Reality and Best Practices
  - forensically speaking…

Correct, Horse Battery, Staple!

http://xkcd.com/936/



Length is everything.

- Go as long as you can 12, 15 and even 20+ characters
- Use a password manager -- choose what matches you best
  - 1Password (personal)
  - LastPass (cloud)
  - iCloud Keychain (personal)
  - simplesafe (self hosted), vaultier.org(self hosted)
- Ok to keep notes in any SSL/encryption protected app: Notes, OneNote, etc…
  - Some people even use secure notes in Keychain
  - Beware of "replacing" the keychain, however

Firewalls

- System that is designed to block unauthorized access while permitting outward communication.
- Often a simply way to keep out nasties
- Built-in to OS X, built into most home routers
- Third party options
  - cisco, barracuda, untangle, smoothwall, pfsense

VPNs: Why you need them

- Basic architecture: virtual private network, secures and encrypts all traffic of a mobile or offsite user
- Simplest implementation for a small business
  - mac server has basic VPN built in.
    - allow offsite users to connect to home network resources
    - geolocation offset (it'll look like you are in the office)
    - casual secure browsing from insecure locations
- Using a router to host a VPN
  - dd-wrt,tomato, pfsense, smoothwall, untangle cisco,

.. a few more things..

.. Servers

- Do you have a backup?.. multiple backups?.. are you sure? how often do you backup? have you tested the backup? How long would it take to recover? offsite backup?
- Who has access to your data? encrypted?
- Is your web server on your primary network?.. does it need to be?
- Do you update your web server regularly? wordpress? drupal? plugins?
- 3rd party software? how secure is it? (target and home depot hacks in 2015 were both caused by 3rd party products)

Your biggest security risk..

Users..

- What access do they need access to? what access do they actually have?
- Are your users working from home? .. How?
- Do your users understand the need for security? do they understand the risks?
- How are they moving data? is it encrypted? are they using personal email, dropbox? thumb drives?
  - *note about SSD's and wiping…
- Do you know your users needs? Do you have an open forum where they can communicate with you and you can communicate with them?
- Do you know your users? especially your IT staff..
- Are they happy? .. are you sure?

More Resources

- https://nakedsecurity.sophos.com/
- https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/
- http://www.thesafemac.com
- https://macviruscom.wordpress.com/
- https://blog.malwarebytes.org/

Questions?



Darrell Miller
darrellrhodesmiller@gmail.com

MACTECH PRO EVENTS