Security.
Keeping them out.

Edward Marczak
marczak@radiotope.com
@marczak

MACTECH

MACTECH

Disclaimer

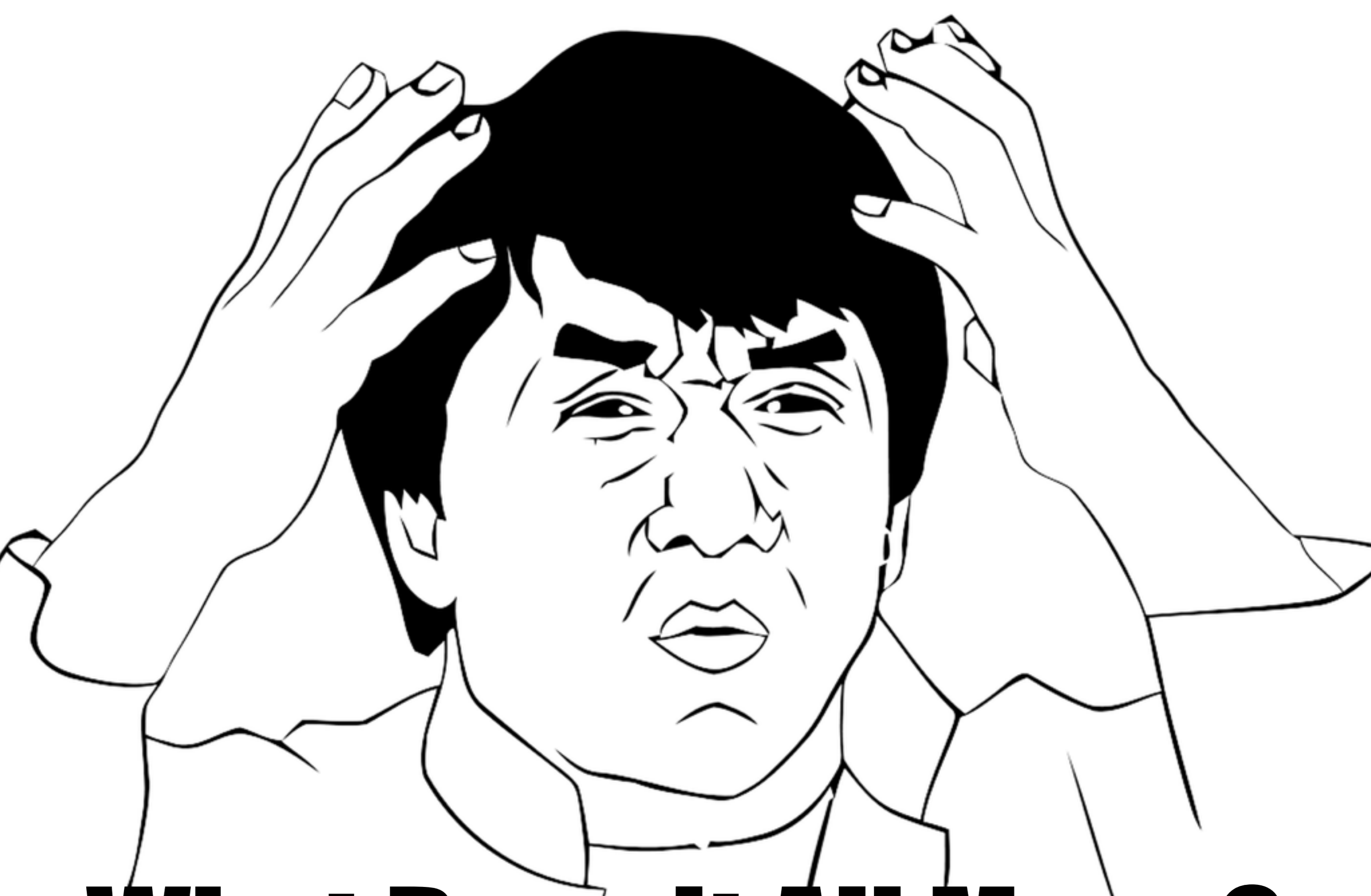
MACTECH

http://macte.ch/mtbcsec

MACTECH

Security

MACTECH



What Does It All Mean?

The human element

- There's nothing that you can do about it.
- They will write their passwords down on a post-it note.
- They will use their street name, 1234, etc...
- All you can do is educate, and inform.
  - Scare tactics don't work.
  - Educate, don't lecture.

?

MACTECH

Thieves: Targeting us?

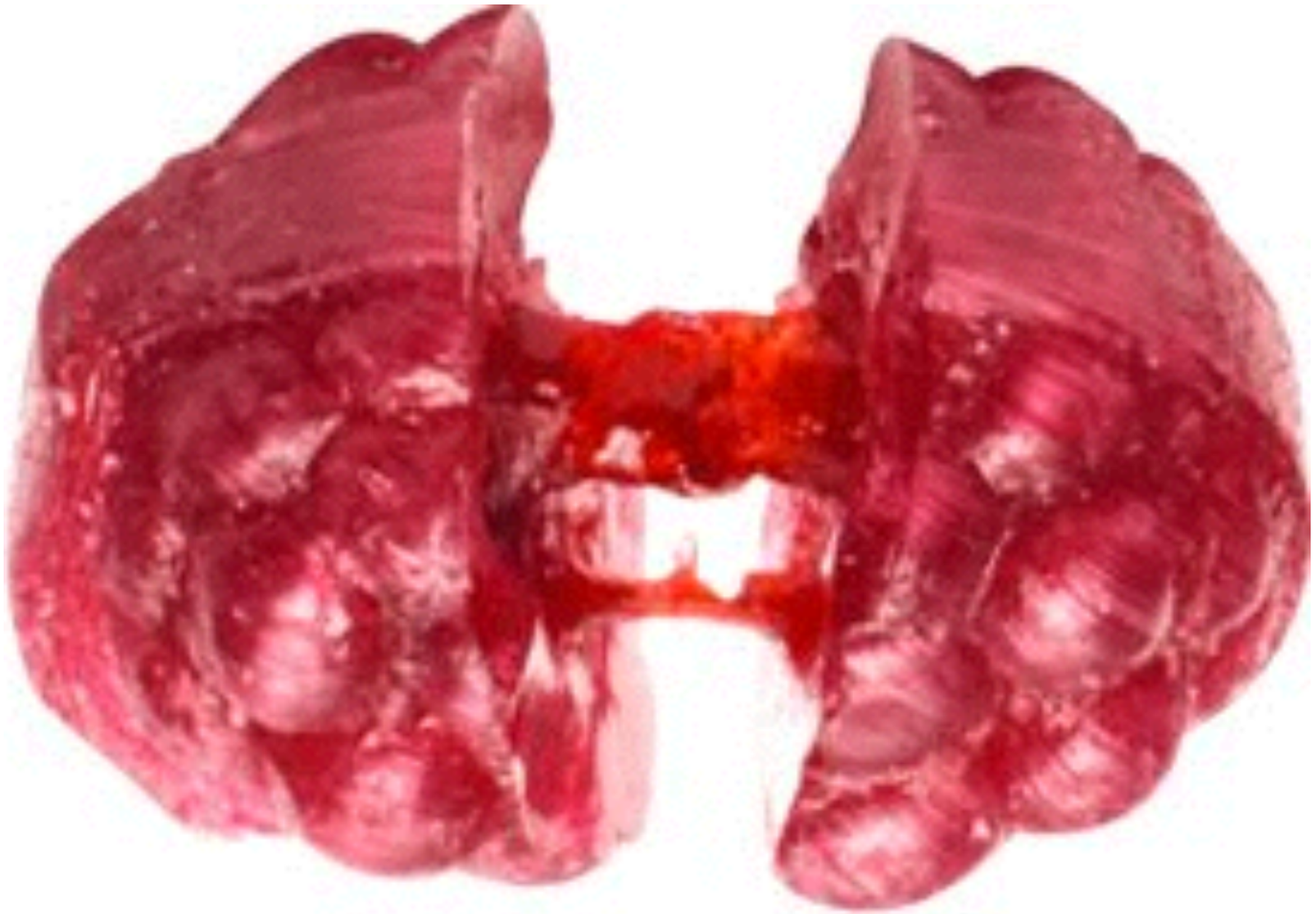
Thieves: Targeting us?

AhhhhhhhYup

MACTECH

?

MACTECH



Keeping them out

MACTECH

Encryption

Network, Servers and Services

- Encrypt everywhere
  - On disk
  - In transit

MACTECH

Two Factor (2FA)

- A second token for authentication
  - "Something you have"
    - Increasingly, this is your phone
- Prevents impersonation

10 Most Common Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123

MACTECH

Source: http://splashdata.com/press/worstpasswords2013.htm

MACTECH

Two Factor (2FA)

- A second token for authentication
  - "Something you have"
    - Increasingly, this is your phone
- Prevents impersonation
- Software or Hardware

Two Factor (2FA)

Software

- SMS
  - Crappiest method
  - This is leaky as people like convenience
- Authy
- Google Authenticator
  - Open Source, Open API
  - Google account: GMail, Docs, Hangouts, Finance, Wallet, etc.

Two Factor (2FA)

Hardware

- YubiKey
- RSA SecurID
- Given one by your provider
- Integration with Apple devices?
  - Kind of

Two Factor (2FA)

Who is doing this?

- Blizzard - battle.net (WoW, Diablo 3, StarCraft 2)
- NCSoft - Guild Wars 2
- Twitter
- Google
- Microsoft
- Facebook
- Apple?

Two Factor (2FA)

Who should be doing this?

- Your bank
- DNS host?
- SSL cert provider?

Two Factor (2FA)

http://twofactorauth.org

MACTECH

Public Key Certificates

- Allows for device identity
  - Diversity is good
  - Make every device unique
- Accessing the network
  - RADIUS/802.11X
- Accessing Services
  - Your service here

MACTECH

Perimeter Firewalls

Meh

MACTECH

Firewalls

Ports to open:

- For ssh, open 22 inbound
- For mail, open 25, 110, 143 and 993 inbound
  - Actually, I'd only open the TLS versions of those
- For web resources, open 80 and 443 inbound
- Outbound?

Firewalls

“There are only so many holes you can poke in a firewall before it’s still doing anything.”

- Me. Right now.

MACTECH

Firewalls

- Reporting?
- Reporting on the right thing!
- Constant monitoring
  - Target…sigh.

MACTECH

MACTECH

VPN

Meh

MACTECH

Front-Ending Services

- Bastion Hosts
  - Use two-factor auth
- Reverse Proxy
  - Virtually any auth you like

MACTECH

Your Hosts

MACTECH

Your Hosts

The easy stuff

- Don't run as admin
  - Don’t *run* as admin.
    - You may still want to provide admin on some level.
- Don’t install (or uninstall) unnecessary crap.
- Keep software up to date

10.9.3 Security Update

CoreServicesUIAgent

Available for: OS X Mavericks 10.9.2

Impact: Visiting a maliciously crafted website or URL may result in an unexpected application termination or arbitrary code execution

Description: A format string issue existed in the handling of URLs. This issue was addressed through additional validation of URLs. This issue does not affect systems prior to OS X Mavericks.

10.9.3 Security Update

CoreServicesUIAgent

Available for: OS X Mavericks 10.9.2

Impact: Visiting a maliciously crafted website or URL may result in an unexpected application termination or arbitrary code execution

Description: A format string issue existed in the handling of URLs. This issue was addressed through additional validation of URLs. This issue does not affect systems prior to OS X Mavericks.

10.9.3 Security Update

ImageIO

Available for: OS X Mavericks 10.9.2

Impact: Viewing a maliciously crafted JPEG image may lead to an unexpected application termination or arbitrary code execution

Description: A buffer overflow issue existed in ImageIO's handling of JPEG images. This issue was addressed through improved bounds checking. This issue does not affect systems prior to OS X Mavericks.

10.9.3 Security Update

ImageIO

Available for: OS X Mavericks 10.9.2

Impact: Viewing a maliciously crafted JPEG image may lead to an unexpected application termination or arbitrary code execution

Description: A buffer overflow issue existed in ImageIO's handling of JPEG images. This issue was addressed through improved bounds checking. This issue does not affect systems prior to OS X Mavericks.

10.9.3 Security Update

Intel Graphics Driver

Available for: OS X Mountain Lion v10.8.5 and OS X Mavericks 10.9.2

Impact: A malicious application can take control of the system

Description: A validation issue existed in the handling of a pointer from userspace. This issue was addressed through additional validation of pointers.

10.9.3 Security Update

Intel Graphics Driver

Available for: OS X Mountain Lion v10.8.5 and OS X Mavericks 10.9.2

Impact: A malicious application can take control of the system

Description: A validation issue existed in the handling of a pointer from userspace. This issue was addressed through additional validation of pointers.

Physical Access

- Can't do *anything* to combat?
  - Encrypt
  - Remote wipe

Device Encryption

- "Full" Disk Encryption ("FDE")
  - Built-in to OS X
  - OS X - fdesetup shell utility
  - Enterprise Key Escrow: Cauliflower Vest
    - Build your own
  - iOS
    - Enable a passphrase/pin

Host-Based Firewall

- Built-in to OS X
  - Application-level
    - Checks the signing cert
  - iOS
    - The magic of no running services

Gatekeeper

- Built-in to OS X
- Allows/disallows based on source

Security & Privacy

Show All

General | FileVault | Firewall | Privacy

A login password has been set for this user — Change Password…

Require password immediately after sleep or screen saver begins

Show a message when the screen is locked — Set Lock Message…

Allow apps downloaded from:

- Mac App Store
- Mac App Store and identified developers
- Anywhere

Click the lock to prevent further changes.

Advanced… ?

Gatekeeper

- Built-in to OS X
  - Allows/disallows based on source
- iOS
  - App Store only

Management Tools

- Management tools should police your nodes
- Your hosts should check-in regularly
  - Reporting
  - Status
  - Alerts

MACTECH

Management Tools

BYOD

- F^%$ that
- Largely not compatible with security
  - Can't entirely control device
  - Legal grey area
  - Wipe device when employee leaves?
- If a company expects employees to perform a task that uses technology, they should supply that technology.

Management Tools

- Anti-Virus?
- F^%$ that
- A/V is dead
- Extra software running (as root/in kernel!) provides a greater attack surface

Management Tools

- Binary White/Blacklisting

What Not to Do

MACTECH

What Not to Do

- Pretend you know what you're doing
  - Really: hire someone that does
- Rely on security by obscurity
- Become complacent
  - Not in your skills/knowledge
  - Not in your platform
    - goto fail

https://lists.apple.com/mailman/listinfo/security-announce

Security.
Keeping them out.

Edward Marczak
marczak@radiotope.com
@marczak

MACTECH

Questions?

Edward Marczak
marczak@radiotope.com
@marczak

MACTECH