Managing Security with the Growing Threat of Malware

MACTECH PRO EVENTS

74bit

Jonathan Spiva

MacAdmins Slack: @jonathan.spiva
Twitter: @jonnyspiva

MACTECH PRO EVENTS

MACTECH PRO EVENTS

74bit

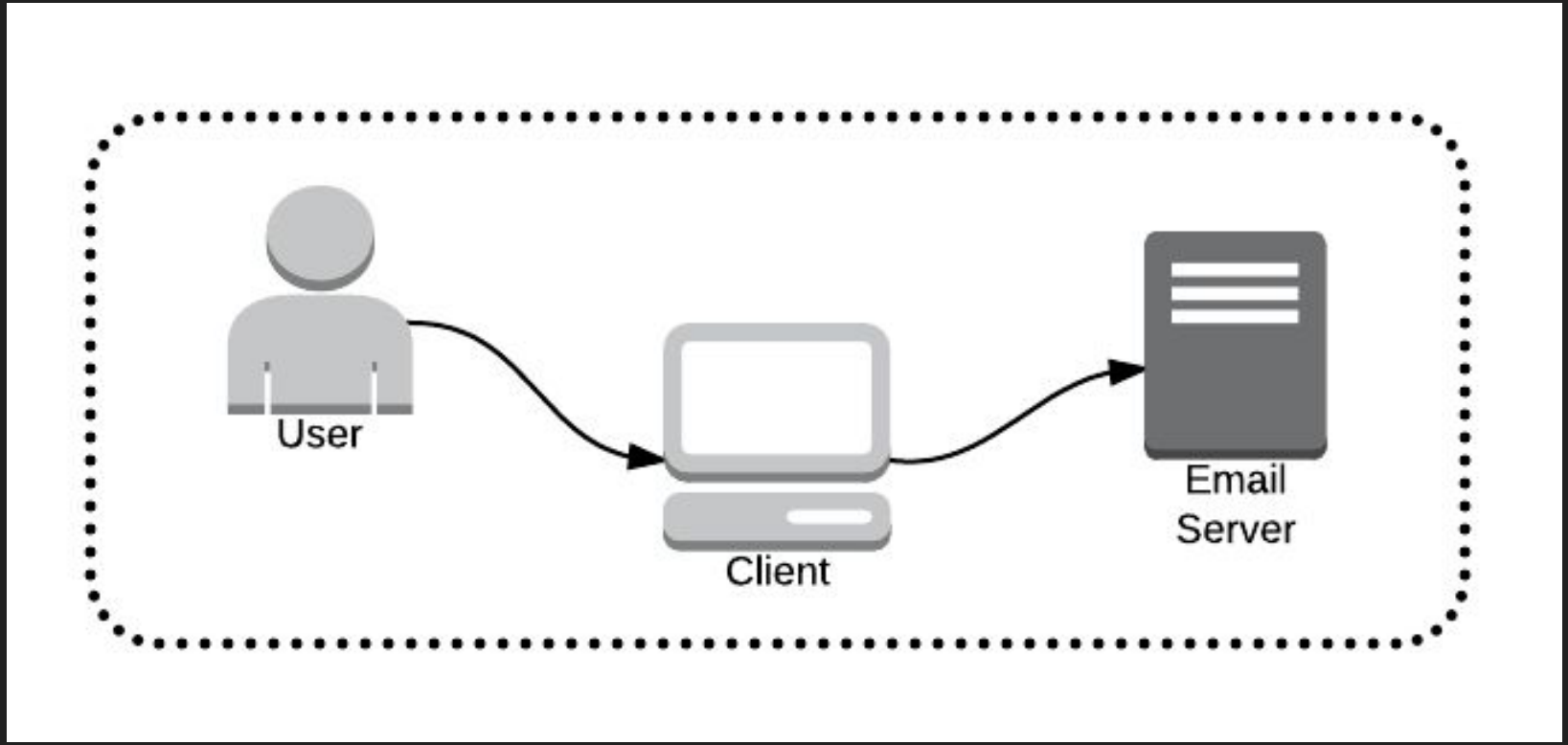
Laying some groundwork

1. What is at risk?
2. The relationship between security and convenience/speed
3. All devices are vulnerable
4. Defining the terms
5. Informal survey

What is at risk?

How does risk affect the entire organization?

Courtesy of Sturgis Buffalo Chip




4K ULTRA HD
HIGHEST RATED TV OF 2015
cnet
9/2/15
amazon
iHeart RADIO
WorkCentre 5845
xerox

virus

A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Source: https://niccs.us-cert.gov/glossary

vulnerability

A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Source: https://niccs.us-cert.gov/glossary

malware

Software that compromises the operation of a system by performing an unauthorized function or process.

Source: https://niccs.us-cert.gov/glossary

spyware

Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Source: https://niccs.us-cert.gov/glossary

phishing

A digital form of social engineering to deceive individuals into providing sensitive information.

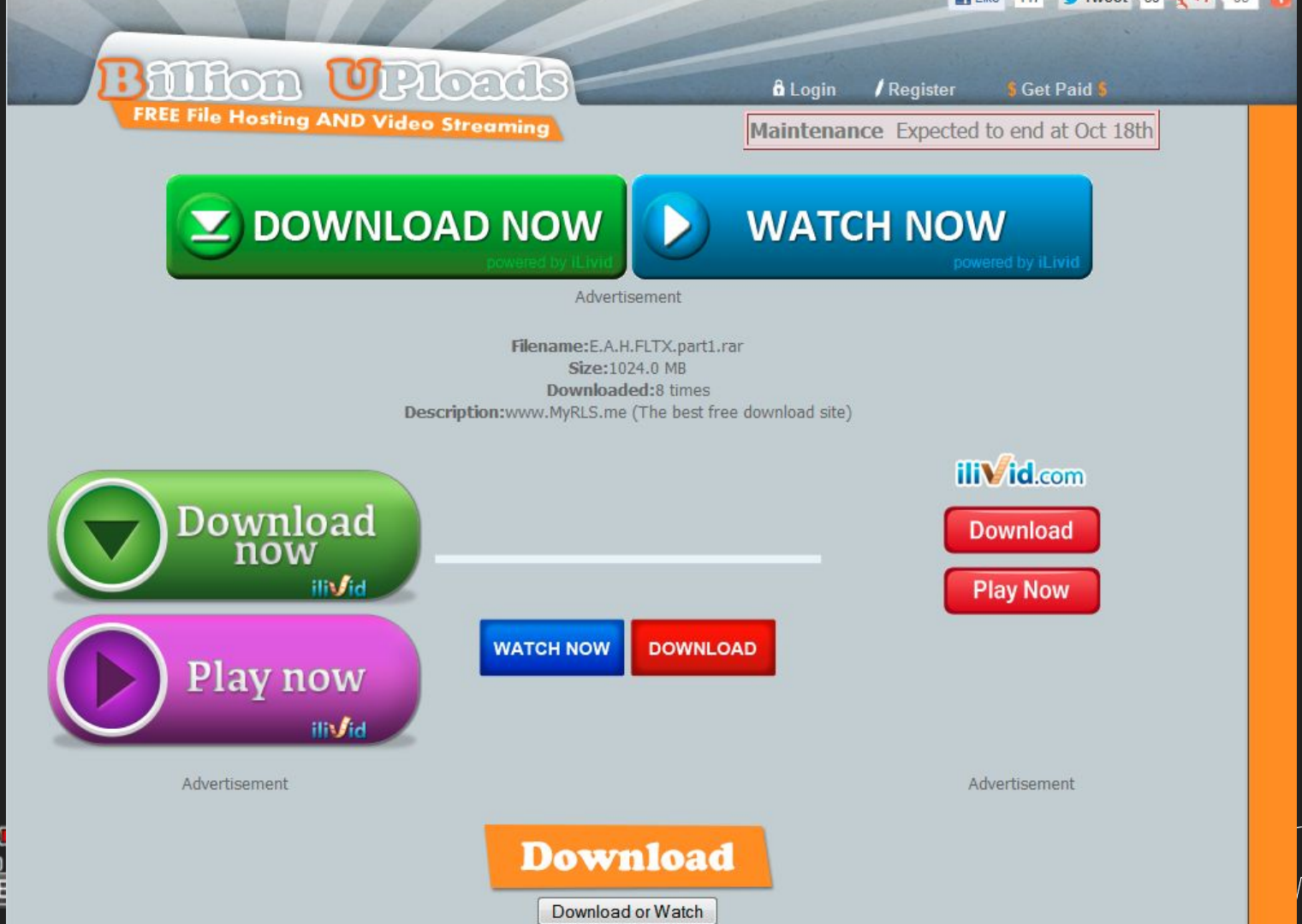
Source: https://niccs.us-cert.gov/glossary

What they have seen in the wild on OS X?

What can we do?

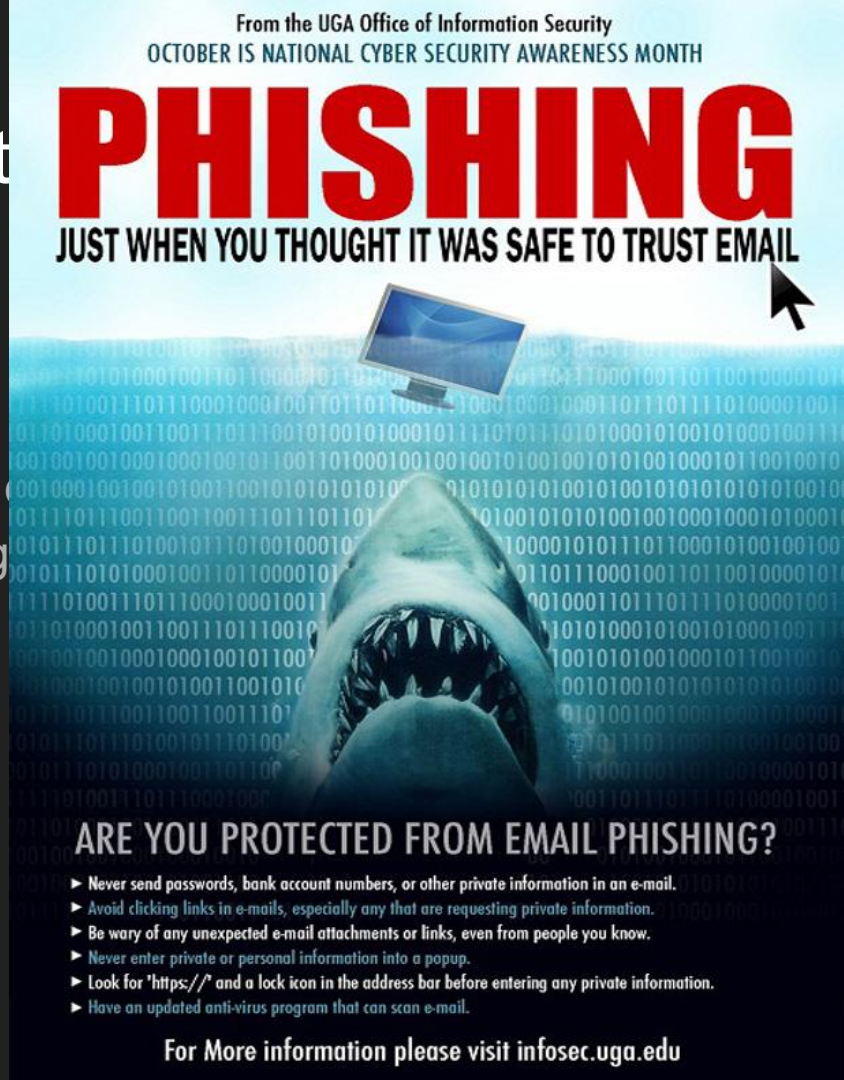
What can we do?

1. Teach your users to fish (not phish)
2. Pilot Error!
3. Understand our own devices
4. Consider different attack vectors


Billion UPloads
FREE File Hosting AND Video Streaming
Login
Register
$ Get Paid $
Maintenance Expected to end at Oct 18th
DOWNLOAD NOW
powered by iLivid
WATCH NOW
powered by iLivid
Advertisement
Filename:E.A.H.FLTX.part1.rar
Size:1024.0 MB
Downloaded:8 times
Description:www.MyRLS.me (The best free download site)
Download now
ilivid
Play now
ilivid
WATCH NOW
DOWNLOAD
ilivid.com
Download
Play Now
Advertisement
Advertisement
Download
Download or Watch

It’s our responsibility to educat

- Get them excited, make securty cool
- Lunch and Learns
- Posters
- Give them real world examples, from your
- Make security part of your “new IT”, saying



MACTECH PRO EVENTS

Pilot Error!

The Apple Tools Are Pretty Good!

- Xprotect (File Quarantine / Known Malware Detection)
- Gatekeeper (Code Signing)
- System Integrity Protection
- FileVault (Full Disk Encryption)
- Firewall
- Standard accounts & Guests accou
- Parental Controls
- Firmware Passwords

Third-party tools feel in some gaps

- Commercial Anti-Virus
- osxlockdown (https://github.com/SummitRoute/osxlockdown)
- MalwareBytes (https://www.malwarebytes.org/business/
- Watchman (https://www.watchmanmonitoring.com/)
- SavingThrow (https://github.com/sheagcraig/SavingThrow)
- Santa (https://github.com/google/santa)
- CarbonBlack (Formerly Bit9, https://www.carbonblack.com/)

Tools for the admin and power users among us.

- BlockBlock (https://objective-see.com/products/blockblock.html)
- LittleSnitch (https://www.obdev.at/products/littlesnitch/)

Reduce risk where you can

- Do you need three browsers on all your computers?
- Do all your computers require Flash?
- Do all your computers require Java?
- Do all your computers require Office?
- Do all your computers require Adobe Acrobat?

Security goes keeper then a OS.

- Unencrypted network traffic
- browser addons / extensions
- EMAIL!
  - SPF, DKIM, DEMARC
- Social engineering still exists.

Our Recipe

The Basics

- Enforce all machines are fully patched and on the most recent OS X version
- No “auto-login”
- Primary users are not admins.
- Devices locks after 3 minutes idle time
- Require password prompt after computer sleep / screensaver
- FileVault enforced on all OS X devices, escrowed individual keys only preferred.
- MDM for remote lock and wipe
- Agent for inventory and remote management
- Email notifications to our helpdesk if a machine's gets out of spec

Deep

- Org-owned SSO system via IdP (Identity Provider) of choice with enforced MFA/2-factor
- Only whitelisted chrome extensions allowed, all others blocked
- No IMAP access to email
- No automatic forwarding of Email messages
- Only the primary user is FileVault-enabled
- Weekly uninstalls of Java and Flash

Things that didn’t fit other places

- https://security.googleblog.com/
- https://vsaq-demo.withgoogle.com
- https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
- http://www.thesafemac.com/
- https://www.ssllabs.com/
- https://www.certificate-transparency.org/
- https://macadmins.org/ #security

Final Thoughts

- Don’t expect your users to follow any security policy you or your team are unwilling to follow yourself.
- There are always exceptions, don’t let a single use case derail your entire organization's security.
- Security is a journey not destination.

Q & A

MacAdmins Slack: @jonathan.spiva
Twitter: @jonnyspiva

MACTECH PRO EVENTS

74bit