Intro to macOS Security

@rrcyrus

SPECTEROPS

Bio

Richie Cyrus (@rrcyrus)

- Senior Analyst @SpecterOps
- Apple Fanboy
- BlackHat Trainer
- Certifications: GCFA, GREM, GCFE, CISSP, etc.

Former:
Apple Inc.
CME Group Inc.
Federal Government

SPECTEROPS

Mac Malware - Believe It

- As the market share goes up, malware authors become more and more interested.
- Mac malware goes way back in time, most notably “Flashback” (2011).
- APT Groups and other threat actors are focusing more on macOS malware.

Mac Malware In The Wild

- 2018:
  - OSX Dummy - Targeting the crypto community.
  - Cryptominer that snuck through the App Store.
  - Coldroot RAT
  - DNS Hijacker

Mac Malware - Open Source

- Pupy RAT - https://github.com/n1nj4sec/pupy
- Evil OSX - https://github.com/Marten4n6/EvilOSX
- Empire - https://github.com/EmpireProject/Empire

SPECTEROPS

macOS Infection Vectors

- Phishing - Watch out for documents with MACros.
- Supply Chain Attacks - Transmission & Handbrake
- User Error - Is that REALLY Adobe Flash??
- Vulnerabilities - #iamroot

Command Line Primer

- whoami
- pwd
- ps aux
- strings
- env
- sw_vers
- file
- less
- grep
- cat
- nano
- plutil
- lsof
- caffeinate
- alias
- Softwareupdate
- lsbom
- lipo

Common Mac File Formats

- Property Lists - .plist (Binary & Normal)
- Applications - .app
- Mach Object file format - Mach-o
- Apple Disk Image - .dmg
- Scripts (.py, .sh, etc.)

What is a plist?

- XML or json format
- Normal .plist file
- Binary .plist file

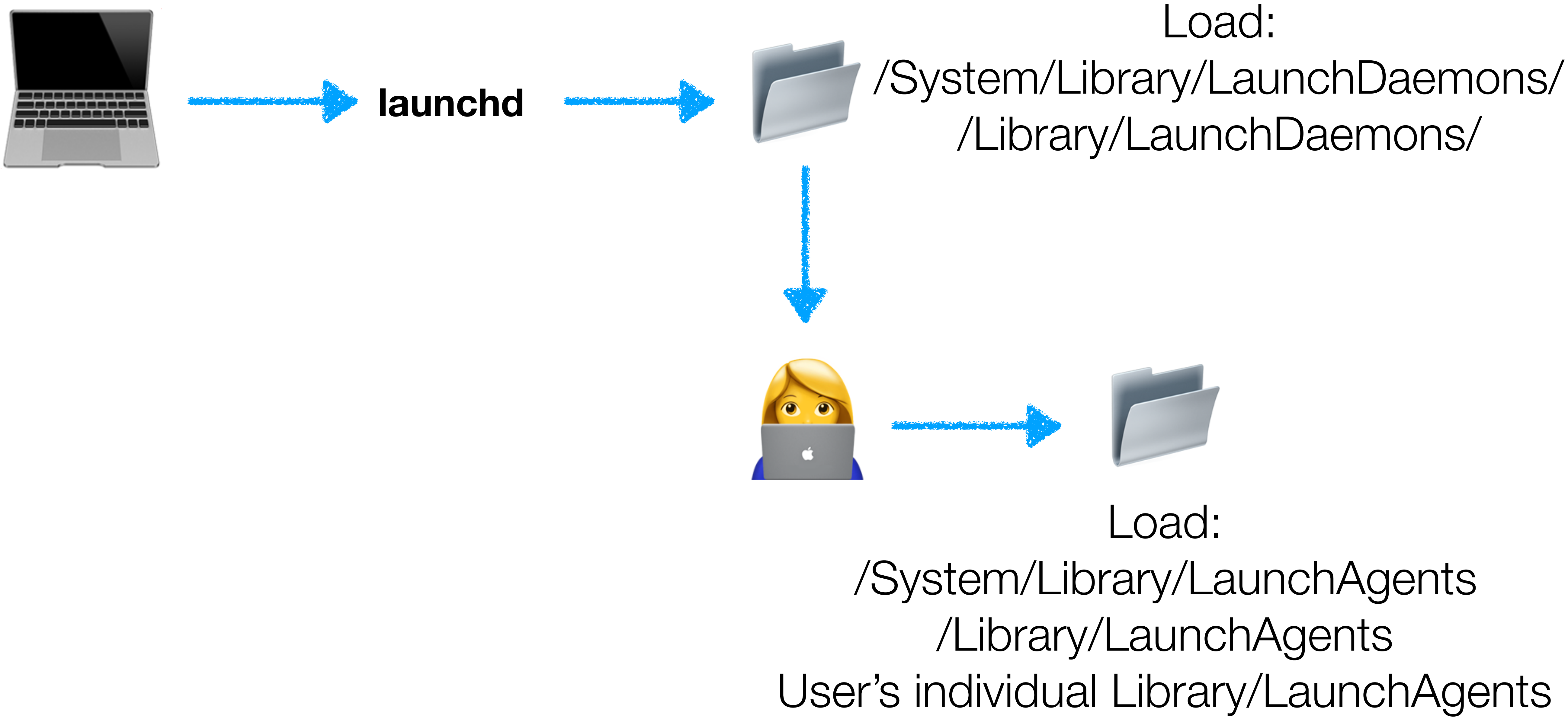
File Format Walkthrough

Artifacts of Malware

- Launch Agents/Daemons
- Cron Jobs
- Files in /tmp
- Browser Extensions
- Kernel Extensions
- Login Items

SPECTEROPS

Launch Agents & Daemons



launchd

Load:
/System/Library/LaunchDaemons/
/Library/LaunchDaemons/

Load:
/System/Library/LaunchAgents
/Library/LaunchAgents
User’s individual Library/LaunchAgents

/tmp

- Bad things happen in /tmp folder.
- Should monitor /tmp every once in a while.

Browser Extensions

- Code that adds functionality to browsers.
- https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses

Kernel Extensions

- Code that is loaded/unloaded into the kernel.
- How to view them?
- https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/

Login Items

- Specific applications designed to run when the user logs in.

- https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

Artifact Walkthrough

Logs of Interest

- System Logs
- Bash History
- Quarantined Items
- Install log
- Command line and GUI (Console.app)

Logs Walkthrough

Sysdiagnose

- System performance issues tool
- Must be run as root
- What does it collect?
  - Top output, crash reports, network status, loaded kernel extensions, system logs and more.
- How do I use it?

Code Signing

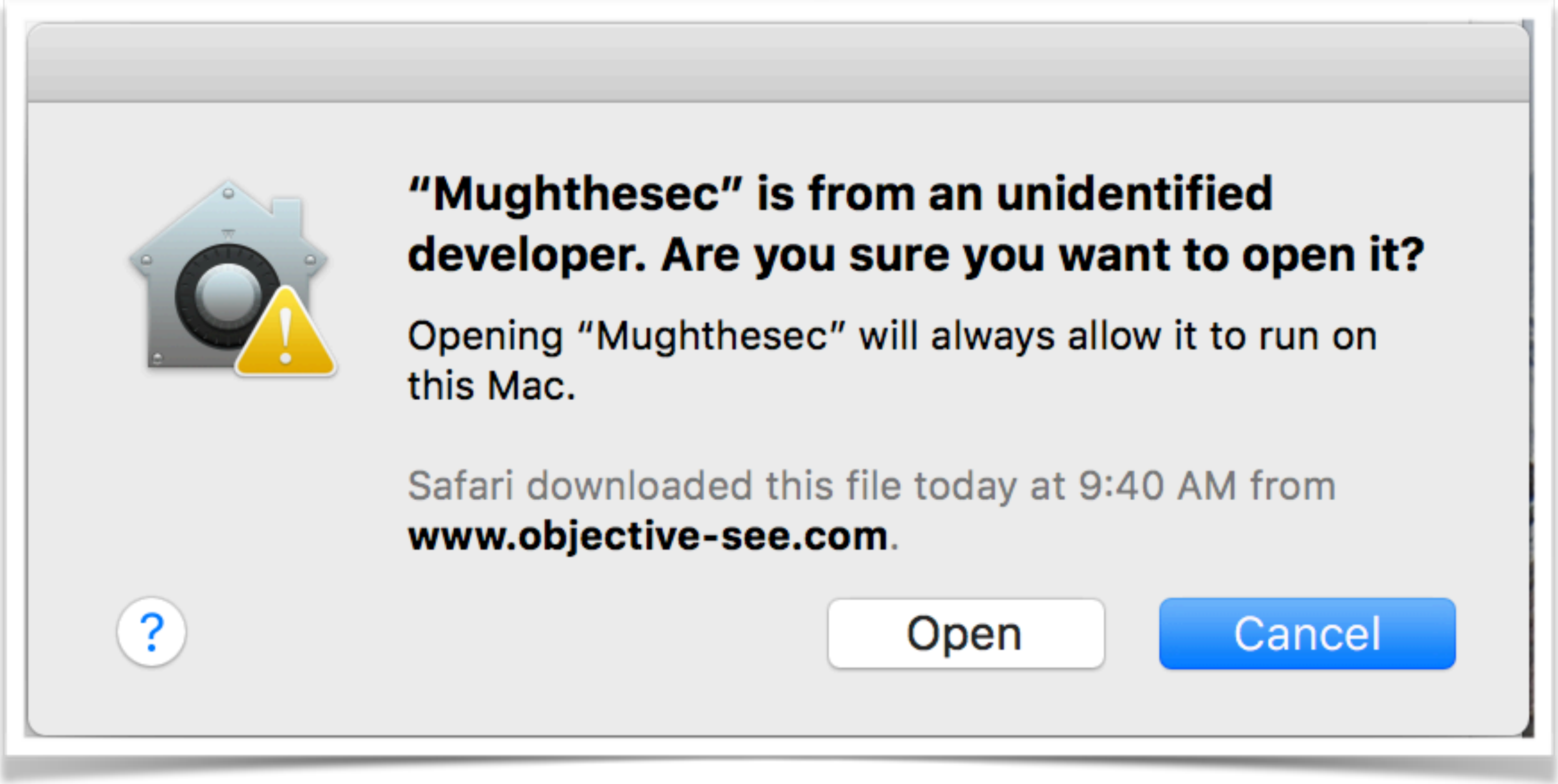
- Codesign tool
- Validate the signatures of binaries on the system
- Also check out attributes and entitlements.

Break

Protect Your Mac

Public Service Announcement About Admin Accounts 😃

Gatekeeper

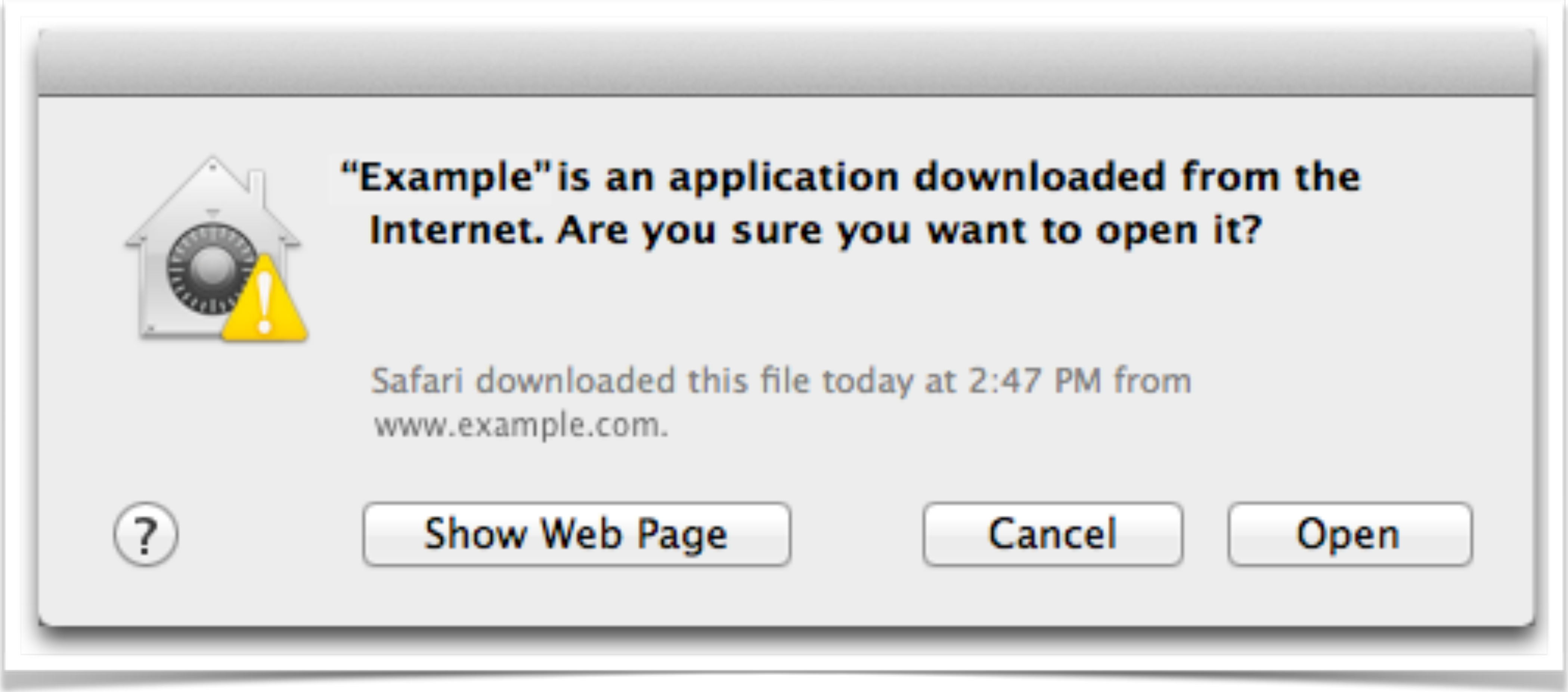


“Mughthesec” is from an unidentified developer. Are you sure you want to open it?

Opening “Mughthesec” will always allow it to run on this Mac.

Safari downloaded this file today at 9:40 AM from **www.objective-see.com**.

File Quarantine



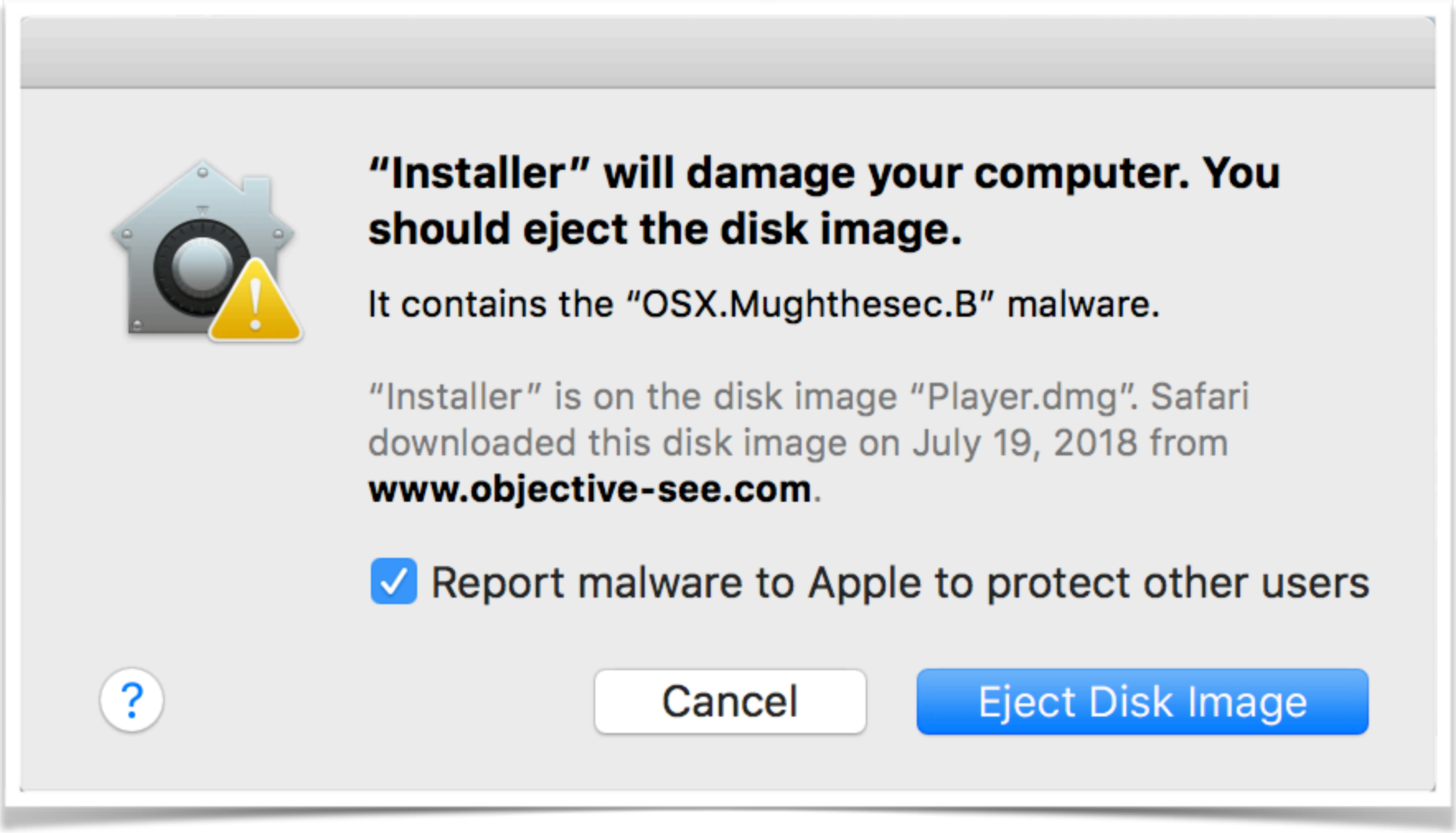
“Example”is an application downloaded from the Internet. Are you sure you want to open it?

Safari downloaded this file today at 2:47 PM from www.example.com.

Extended Attributes

- How does file quarantine know the file was downloaded from the internet?
- How do we see extended attributes?

XProtect



“Installer” will damage your computer. You should eject the disk image.

It contains the “OSX.Mughthesec.B” malware.

“Installer” is on the disk image “Player.dmg”. Safari downloaded this disk image on July 19, 2018 from **www.objective-see.com**.

☑ Report malware to Apple to protect other users

System Integrity Protection

- Rootless operating system
- Even as the root user, you as user are limited to what you can do
- Prevents unauthorized modification of important files and folders on your system

Malware Removal Tool

- Built in tool
- Removes previously identified malware
- Have to enroll in automatic updates
- Update occurs -> Reboot -> Malware gone.
- Not able to get much info unlike XProtect.

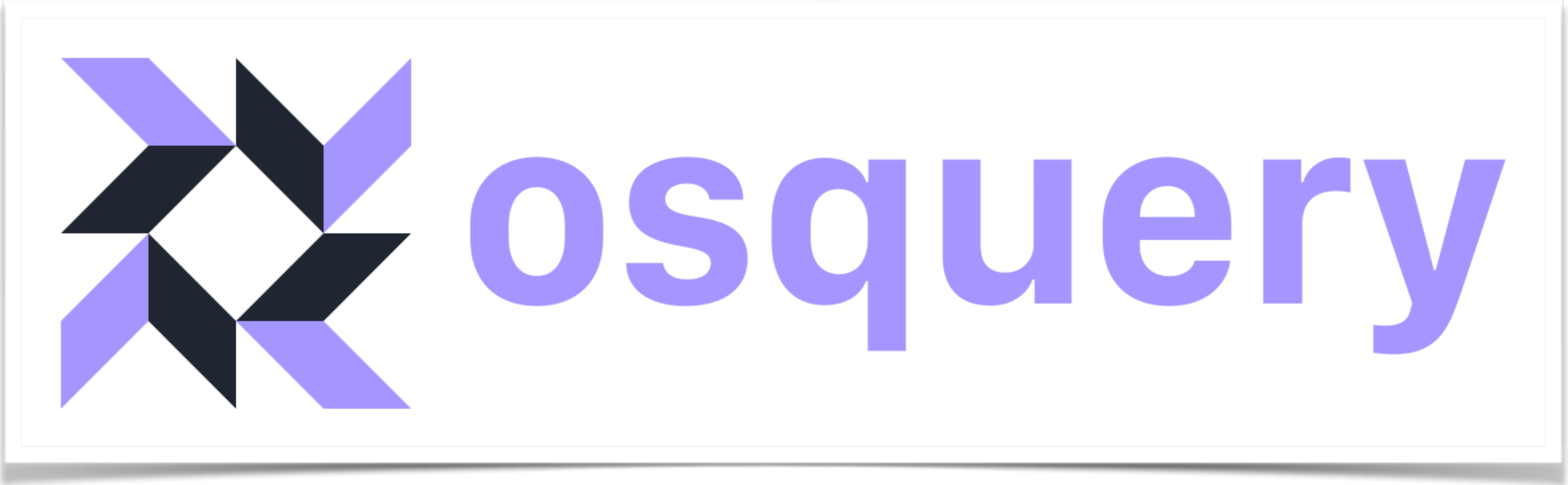
Objective See Tools

- https://objective-see.com/products.html
- Lulu
- Knock Knock
- BlockBlock
- OverSight

Github Guides

- https://github.com/drduh/macOS-Security-and-Privacy-Guide
- https://github.com/0xmachos/mOSL

osquery



- File Integrity Monitoring
- Scheduled queries (Enterprise sweeps)
- Yara Scanning
- Process Monitoring

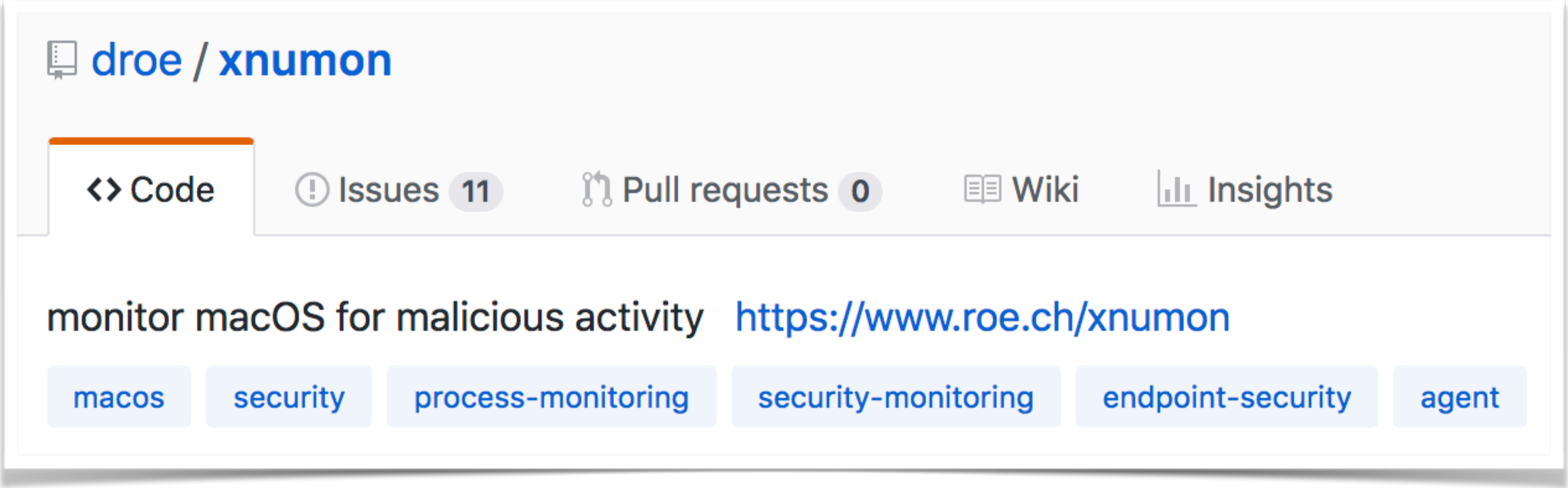
OSX Collector

- Scan a system you suspect may be compromised.
- Scan periodically and send to a SIEM.
- Python Based

Santa

- Kernel Extension
- Application Whitelisting via Whitelisting/Blacklisting
- Process Monitoring

XNUmon



droe / xnumon

monitor macOS for malicious activity https://www.roe.ch/xnumon

- Sysmon for Macs
- Logging of persistent items
- Process Monitoring

Resources - Social Media

Twitter:

- @objective_see
- @patrickwardle
- @iamevltwin
- @thomasareed
- @xorrior
- @howardnoakley

Slack: MacAdmins Group

https://macadmins.herokuapp.com/

Resources - Books/Courses

- OS X Incident Response: Scripting and Analysis by Jaron Bradley

- MacOS and iOS Internals, Volume III: Security & Insecurity by Jonathan Levin

- Course - SANS FOR518: Mac and iOS Forensic Analysis and Incident Response by Sarah Edwards

References Used for Workshop

- https://attack.mitre.org/wiki/Mac_Technique_Matrix
- objective-see.com
- https://developer.apple.com

Objective By The Sea

a Mac Security Conference
in Maui, Hawaii

Nov. 3rd-4th 2018