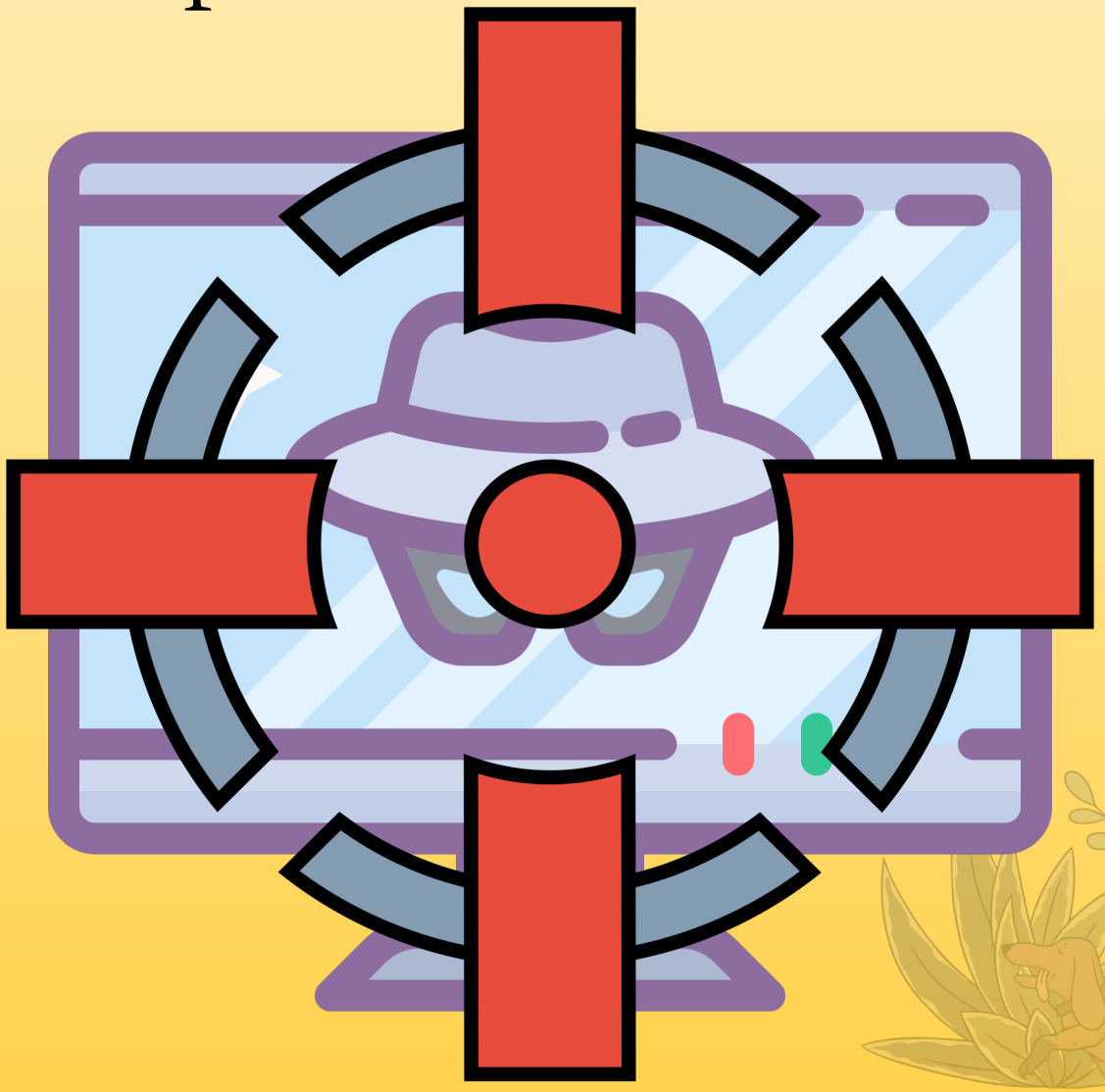
Investigating Macs at the Speed of Compromise

Tim Crothers

The Need for Speed…



Basic OSX

/System/Library/CoreServices/XProtect.bundle/Contents/Resources/XProtect.yara

.dmg – Apple disk image

.kext – Equivalent of driver for OSX – actually a directory

.plist – Property list files

/usr/libexec/PlistBuddy -x -c "Print" *filename*.plist

.app – Application – actually a directory as with .kext

.dylib – Dynamic library file (e.g. Windows DLL)

.pkg – Package (e.g. Linux .tar)

Is There Malz?

- Basic system information
- Memory capture & analysis
- File system analysis
- Running processes
- Connecting externally
- Persistence
- Browser history
- System logs

Basic system information

system_profiler -xml -detaillevel full > system_profil.spx

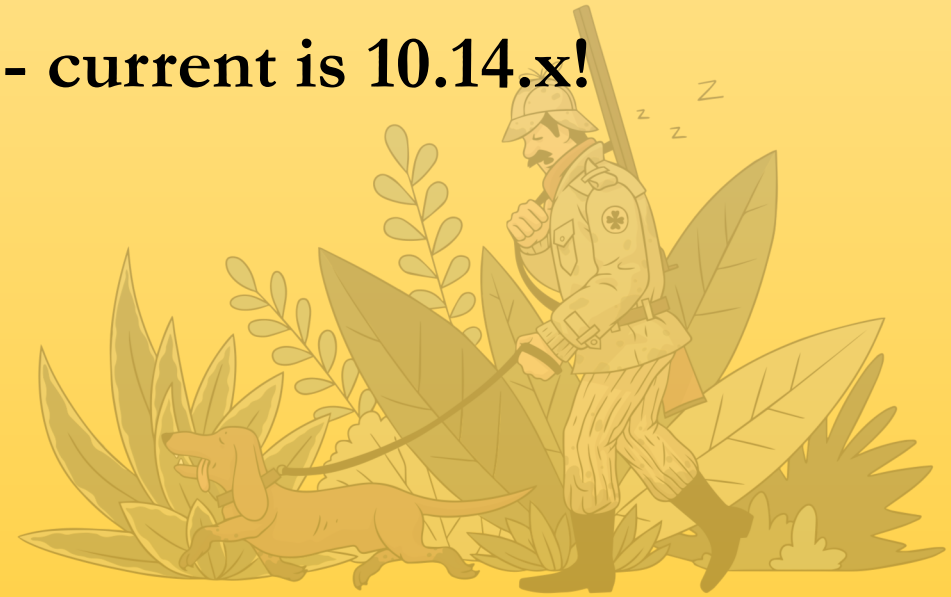
Open with “System Information.app”

Memory capture & analysis

Rekall - https://github.com/google/rekall

Volatility - https://github.com/volatilityfoundation/volatility

NOTE – Both only support through 10.12.x - current is 10.14.x!



File system analysis

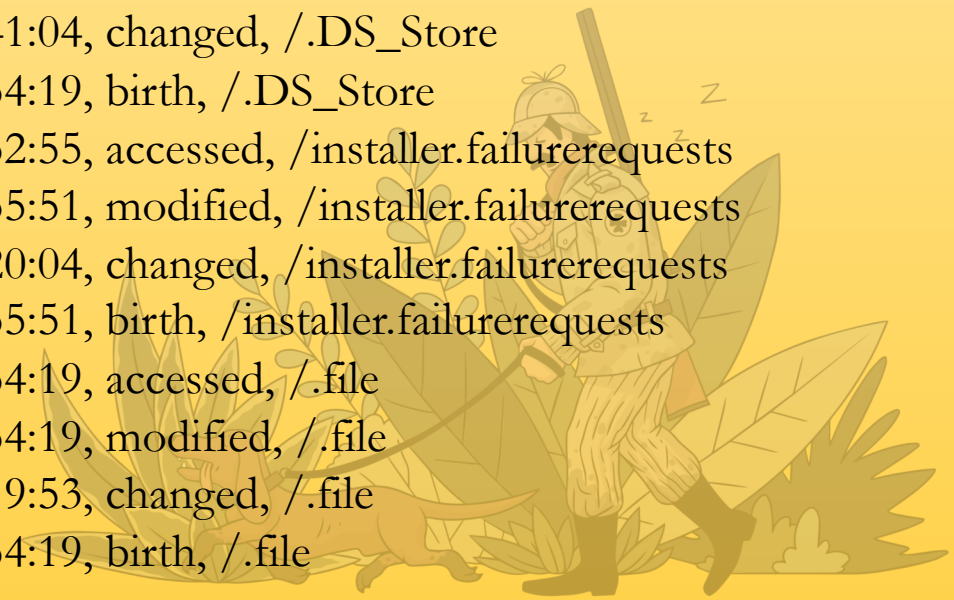
file_walker.py – "OS X Incident Response Scripting and Analysis"
github.com/jbradley89/osx_incident_response_scripting_and_analysis

fileinfo.txt

/.DS_Store, 664, file, 0, 80, 10244, None
/installer.failurerequests, 644, file, 0, 0, 313, None
/.file, 000, file, 0, 80, 0, None
/.OSInstallerMessages, 644, file, 0, 0, 1776, None
/usr/bin/uux, 555, file, 4, 0, 97760, None
/usr/bin/cpan, 755, file, 0, 0, 811, None
/usr/bin/BuildStrings, 755, file, 0, 0, 18320, None
/usr/bin/loads.d, 755, file, 0, 0, 1936, None
/usr/bin/write, 555, file, 0, 4, 23936, SETGID

filetimeline.txt

2019-10-02T02:59:49, accessed, /.DS_Store
2019-09-26T12:41:04, modified, /.DS_Store
2019-09-26T12:41:04, changed, /.DS_Store
2018-08-17T21:54:19, birth, /.DS_Store
2019-09-17T10:52:55, accessed, /installer.failurerequests
2018-08-18T00:55:51, modified, /installer.failurerequests
2018-10-22T16:20:04, changed, /installer.failurerequests
2018-08-18T00:55:51, birth, /installer.failurerequests
2018-08-17T21:54:19, accessed, /.file
2018-08-17T21:54:19, modified, /.file
2018-10-22T16:19:53, changed, /.file
2018-08-17T21:54:19, birth, /.file



File system analysis

Key directories-

/Applications – User wide applications
/Library – Application preferences, configurations, and logs
/System – OSX operating system core files
/User – Equivalent of /home for Linux
/Volumes – Mounted drives
/.vol – Files by inode
/private – Many other directories actually symbolic links to directories here

/bin, /usr, /cores, /sbin, /dev, /etc, /tmp, /var – Equivalent to Linux use

File system analysis

.DS_Store – Holds attributes and customizations like icons per directory

.Spotlight-V100 – In each volume root – contains index information for spotlight

.metadata_never_index – If in volume root tells Spotlight not to index the volume

<*foldername*>.noindex – Folder or file name with this extension tells Spotlight not to index the folder or file

File system analysis

xattr *filename*

mdls *filename* – Metadata about file

stat *filename*

file *filename*

File system analysis

Quarantine

/Users/*username*/Library/Preferences/com.apple.LaunchServices.QuarantineEvents.V2

Maintained by XProtect and includes the majority of downloaded files

Running processes

ps aux

Connecting externally?

netstat -an

lsof –i

Persistence

/Users/$USER/Library/Preferences/com.apple.loginitems.plist
/Application/<application>.app/Contents/Library/LoginItems/
/Library/LaunchAgents
/Library/LaunchDaemons
/System/Library/LaunchAgents
/System/Library/LaunchDaemons
/Users/$USER/Library/LaunchAgents
crontab -l
Kernel extensions (kext)
    /System/Library/Extensions
    /Library/Extensions
    kextstat
/private/var/at/jobs/

Browser history

General

/tmp

/var/tmp

/Users/*username*/Library/Caches/Java/tmp

/Users/*username*/Library/Caches/Java/cache ← Has the IDX and JAR files

IDX parser – https://github.com/Rurik/Java_IDX_Parser

Safari

/Users/*username*/Library/Safari/History.plist

/Users/*username*/Library/Safari/Downloads.plist

/Users/*username*/Library/Safari/LastSession.plist

/Users/*username*/Library/Caches/com.apple.Safari/Webpage Prviews/

/Users/*username*/Library/Caches/com.apple.Safari/Cache.db

Browser history

Google Chrome

/Users/*username*/Library/Application Support/Google/Chrome/Default/History

SELECT datetime(((v.visit_time/1000000) - 11644473600), 'unixepoch'), u.url FROM visits v INNER JOIN urls u ON u.id = v.url;

SELECT datetime(d.start_time/1000000-11644473600, 'unixepoch'), dc.url. d.target_path, d.danger_type, d.opened FROM d INNER JOIN downloads_url_chains dc ON dc.id = d.id;

Firefox

/Users/$USWR/Library/Application Support/Firefox/Profiles/<PROFILE>.default/places.sqlite

SELECT datetime(hv.visit_date/1000000, 'unixepoch') as dt, p.url FROM moz_historyvisits hv INNER JOIN moz_places p ON hv.place_id ORDER by dr ASC;

sqlite3 places.sqlite "select * FROM moz_annos:"

System logs

ASL - Apple System Logs

/private/var/log/asl/

View with either Console.app or syslog

YYYY.MM.DD.[UID].[GID].asl

syslog –d /private/var/log/asl/

syslog –T utc –F raw –d /private/var/log/asl/

Audit logs

/private/var/audit/

StartTime.EndTime – YYYYMMDDHHMMSS. YYYYMMDDHHMMSS

praudit –xn /private/var/audit/*

System logs

Local terminal

login[pid]: USER_PROCESS

login[pid]: DEAD_PROCESS

Login window

loginwindow[pid]: USER_PROCESS

loginwindoe[pid]: DEAD_PROCESS

SSH

sshd[pid]: USER_PROCESS

sshd[pid]: DEAD_PROCESS

Screen sharing

screensharingd: Authentication: SUCCEEDED

System logs

SU

su: BAD SU *username* to root on …

su: *username* to root on …

SUDO

sudo: *username*: TTY=…; PWD=…; USER=root; COMMAND=…

Demo

Other options

- GRR – Google Rapid Response - https://github.com/google/grr
- OSQuery - https://github.com/osquery/osquery

Reference Materials

Sarah Edwards Blog - https://www.mac4n6.com/

Sniper Forensics - https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493922006.pdf

OSXCollector - https://github.com/Yelp/osxcollector

OSX Incident Response - Jaron Bradley - https://github.com/jbradley89/osx_incident_response_scripting_and_analysis

https://developer.apple.com/

Mac OSX Internals – Amit Singh

https://github.com/Marten4n6/EvilOSX

Thank You!

https://github.com/soinull/investigatingmacs

linkedin.com/in/tim-crothers-5458738/