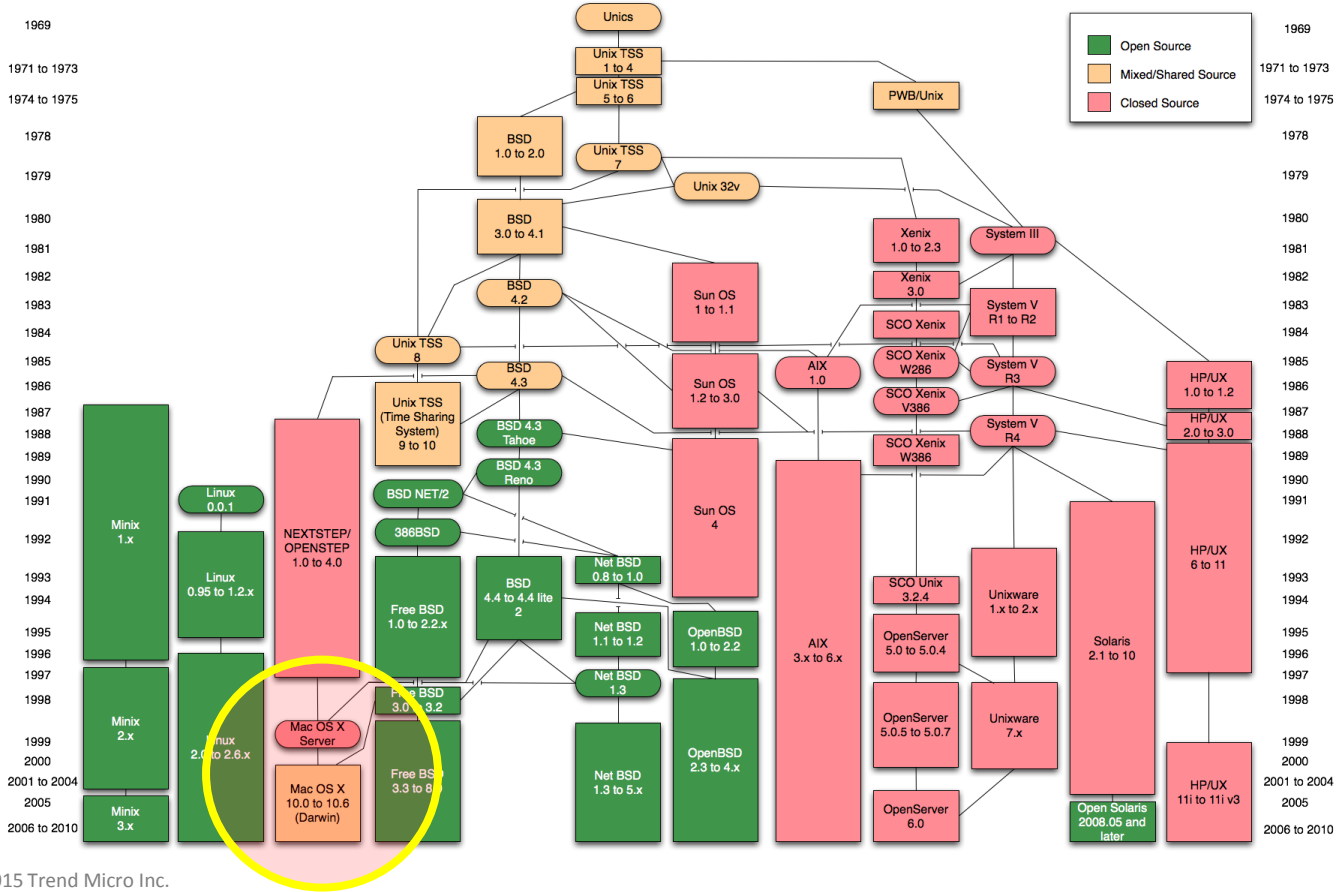
Shifting Paradigms from Windows to Mac

Nicholas Ramos and Michelle Morales

Introduction to MAC OS X

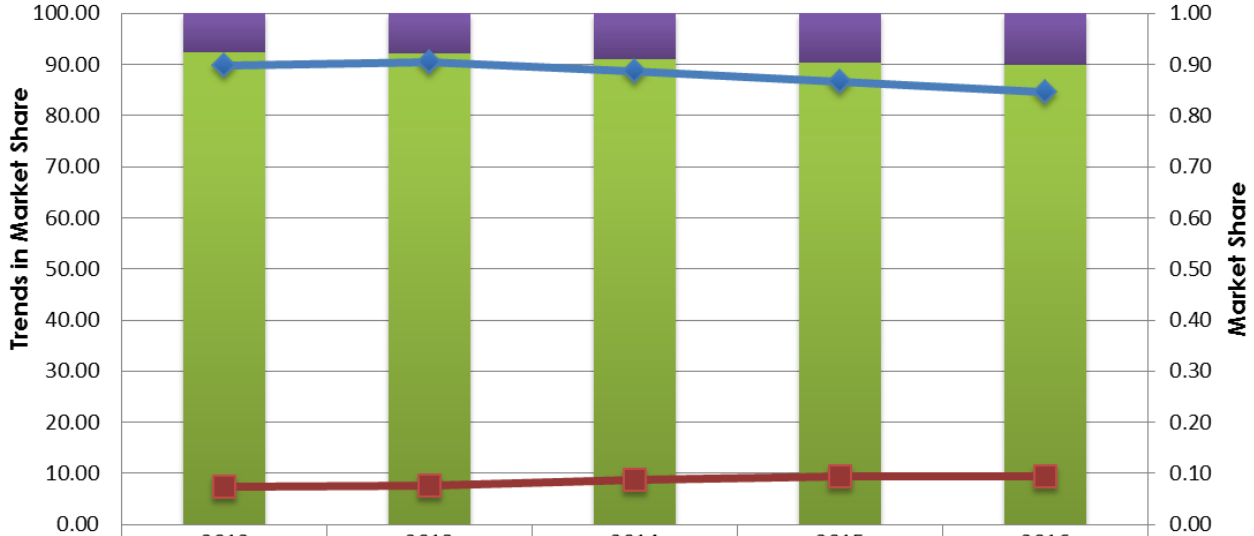
Review



MAC OS X Timeline

Getting to Know More

MAC vs. Windows



	2012	2013	2014	2015	2016
MAC_MS	0.08	0.08	0.09	0.10	0.10
Windows_MS	0.92	0.92	0.91	0.90	0.90
Windows	89.69	90.34	88.66	86.68	84.53
MAC	7.48	7.68	8.76	9.33	9.52

*Market share data is only between Mac and Windows, other operating systems are excluded
*Reference: *http://www.statista.com/statistics/218089/global-market-share-of-windows-7/*

Myths about MAC

MAC can't get viruses

- Yes!! There are incidents and there will more to come.

MAC are safer to use compared to windows

- "Mac OS X software has more high-risk vulnerabilities than all versions of Windows put together," -Bogdan Botezatu

MAC don't crash

- MAC applications crash more than often than in Windows 7 (Network World)

OS X Safety Features

XProtect

- Built-in anti-malware software

GateKeeper

- Halts unauthorized binary execution

Sandboxing

- Prevents user apps from accessing Kernel/core level components

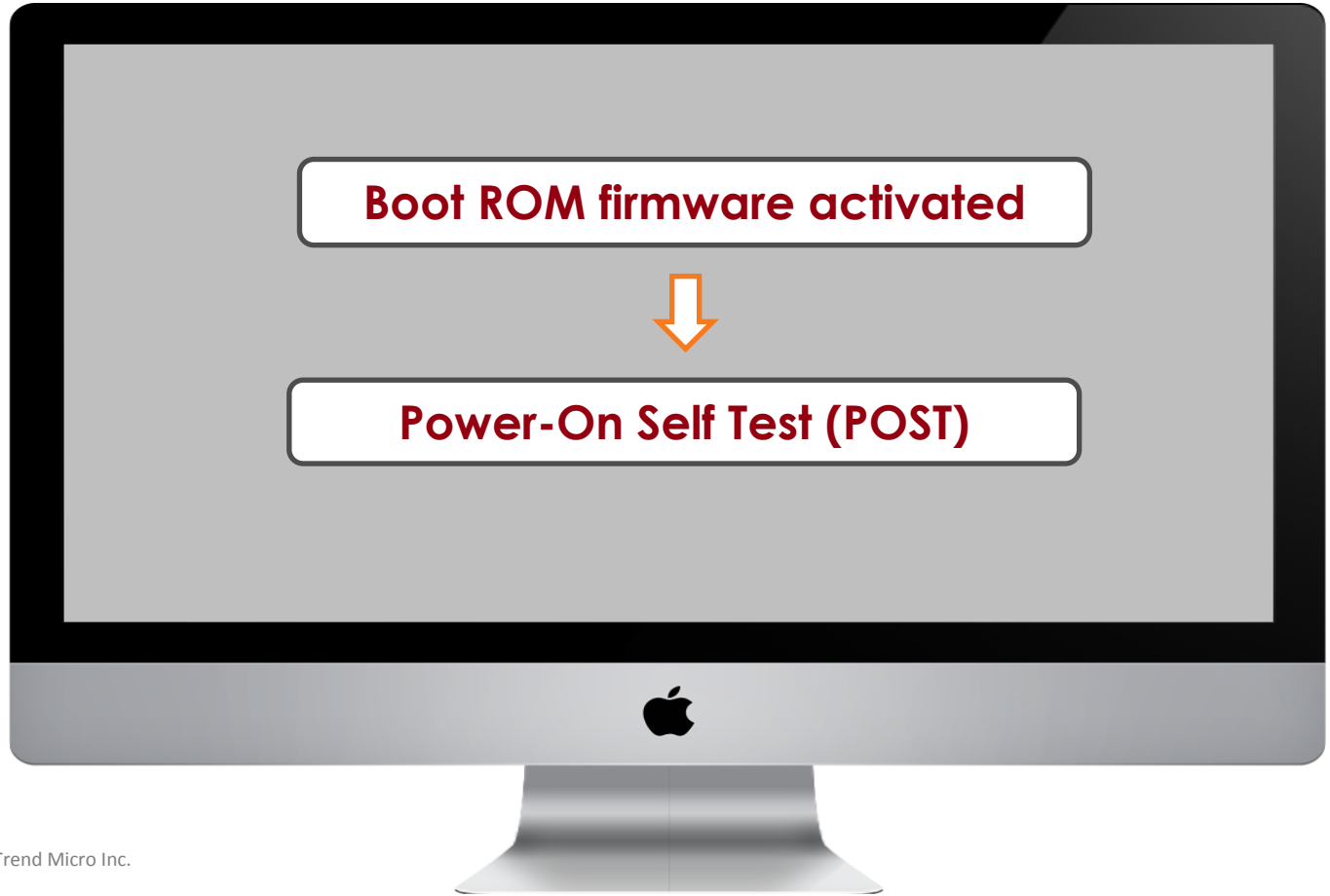
Code Signing

- Only signed kext (drivers) can be loaded

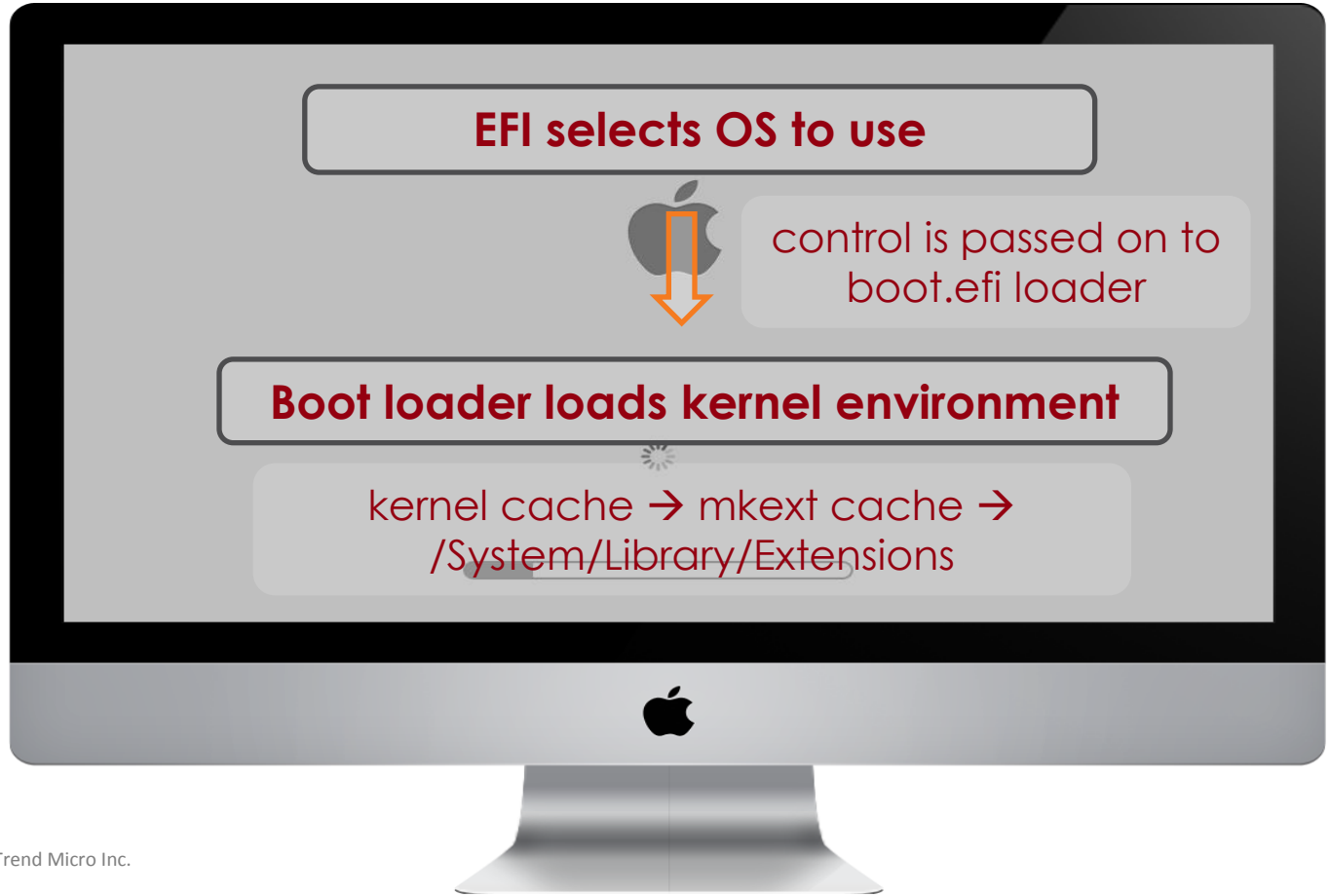
OS X Boot-up Process

MAC Boot-Up

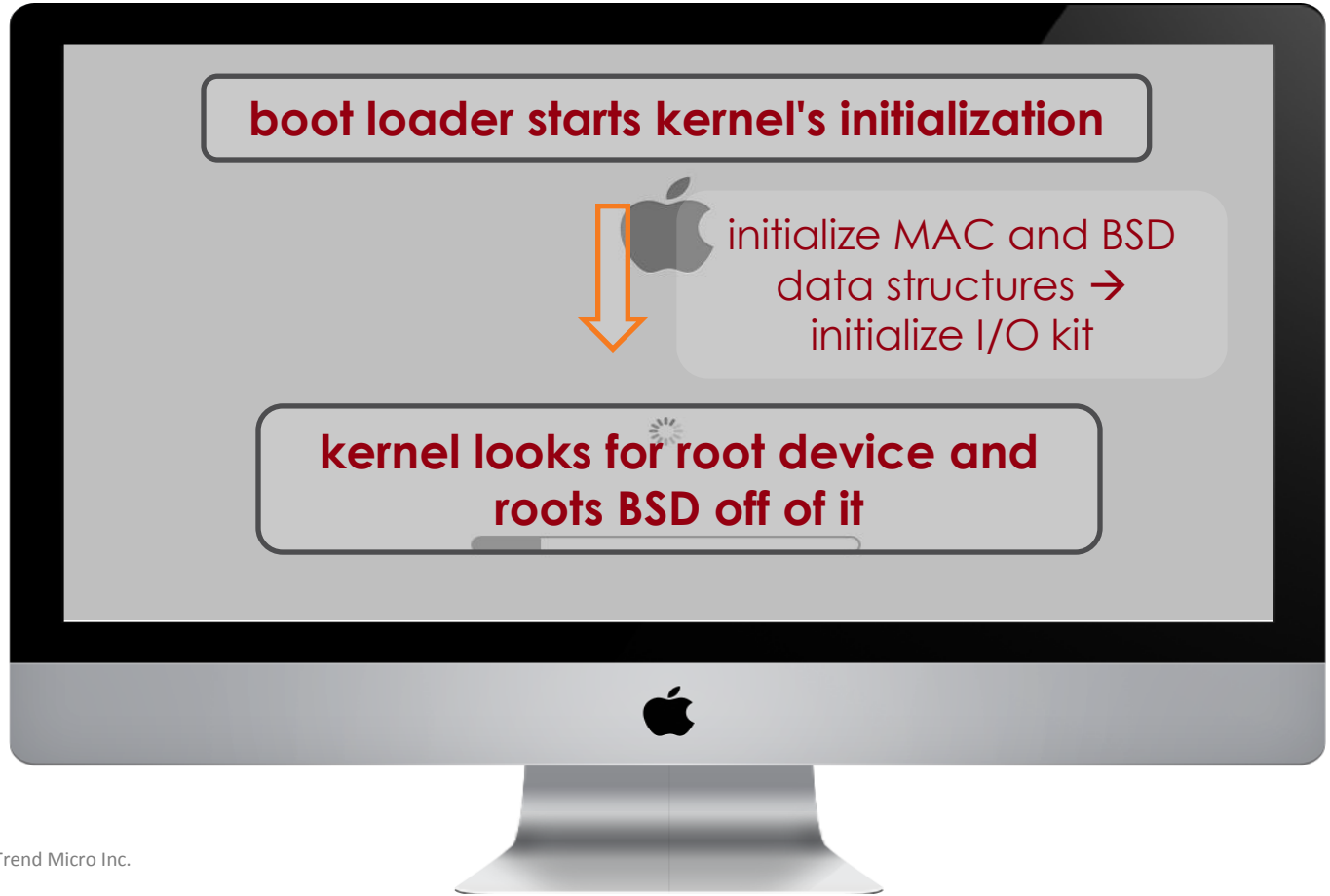
MAC Boot-Up



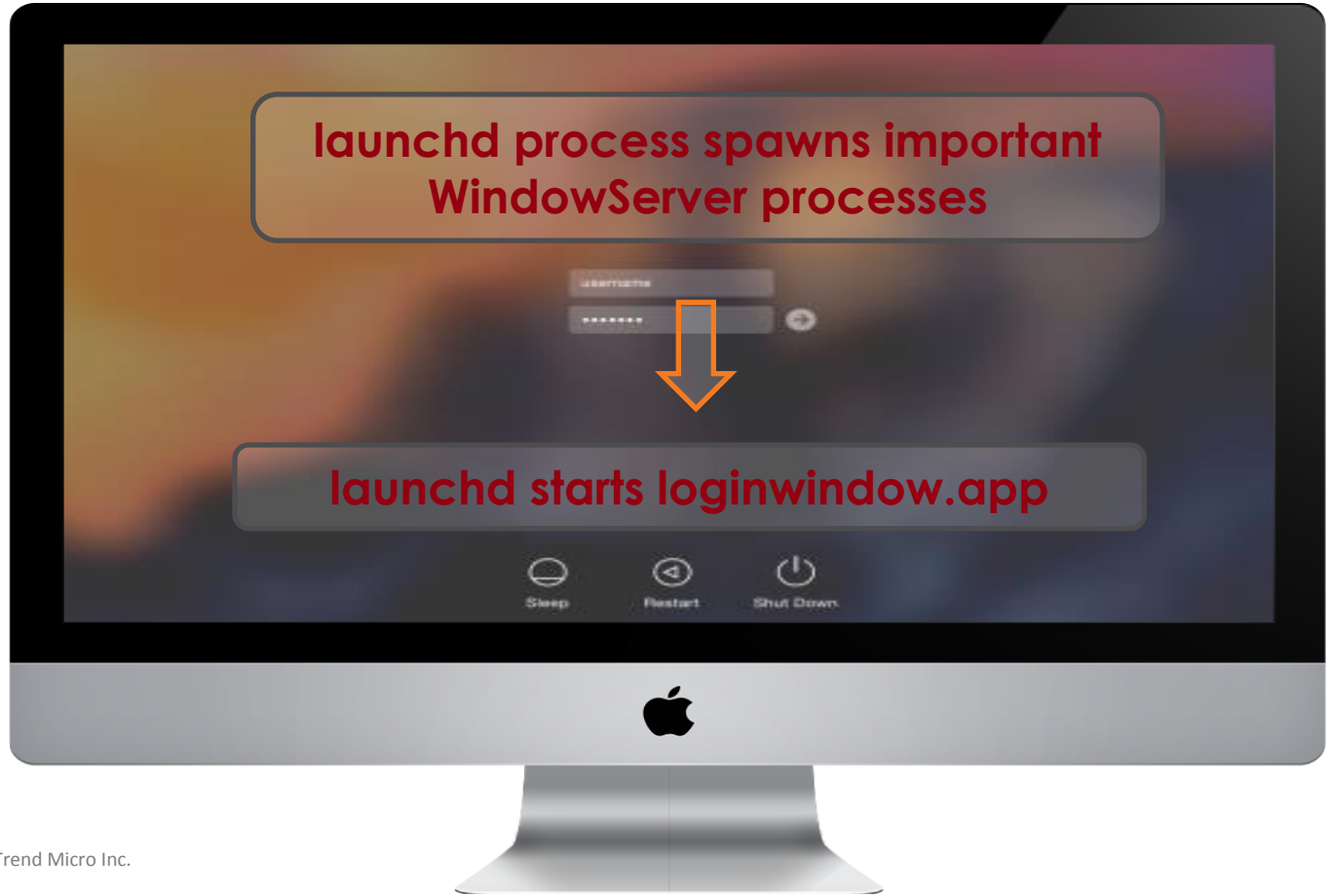
MAC Boot-Up



MAC Boot-Up



MAC Boot-Up

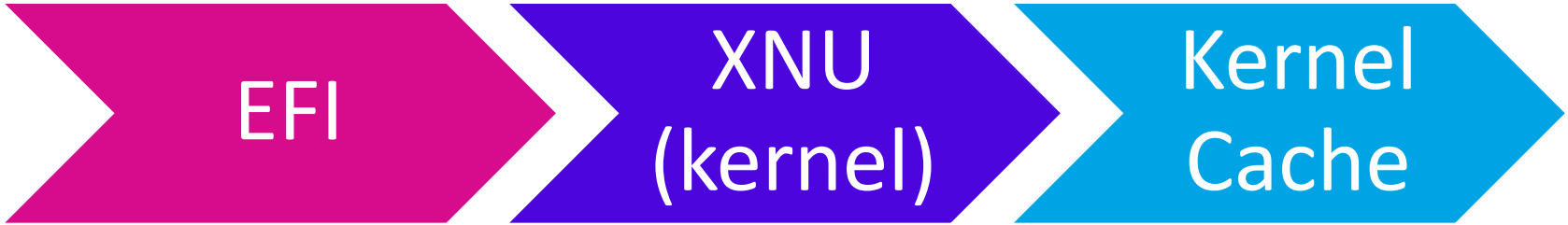


MAC Boot-Up

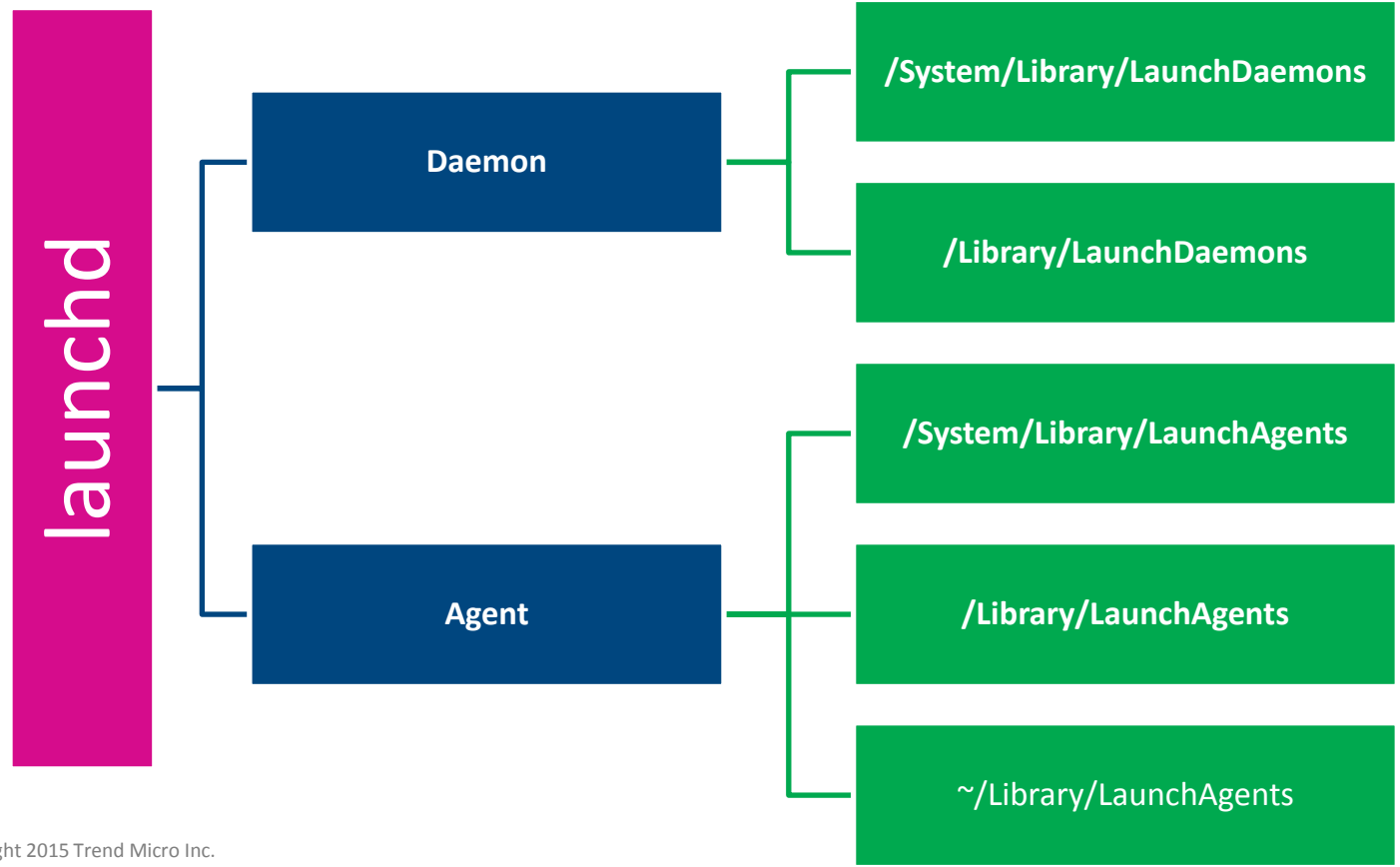
Auto-Start Mechanism

TRICKS AND WAYS FOR MALWARE PERSISTENCE

Pre-Login Persistence



Launched as Daemon or Agent

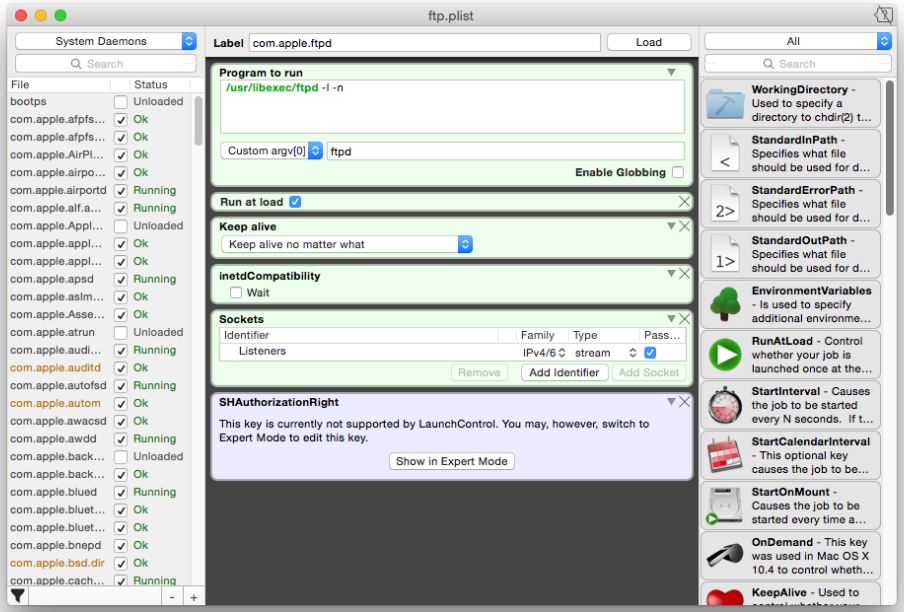


Type of Launched Daemons and Agents

Type	Location	Run on behalf of	Purpose
User Agents	~/Library/LaunchAgents	Currently logged in user	Third-Party App for Specific user
Global Agents	/Library/LaunchAgents	Currently logged in user	Third-Party App for all users
Global Daemons	/Library/LaunchDaemons	root	Third-Party App for all users
System Agents	/System/Library/LaunchAgents	Currently logged in user	Crucial for the OS
System Daemons	/System/Library/LaunchDaemons	root	Crucial for the OS

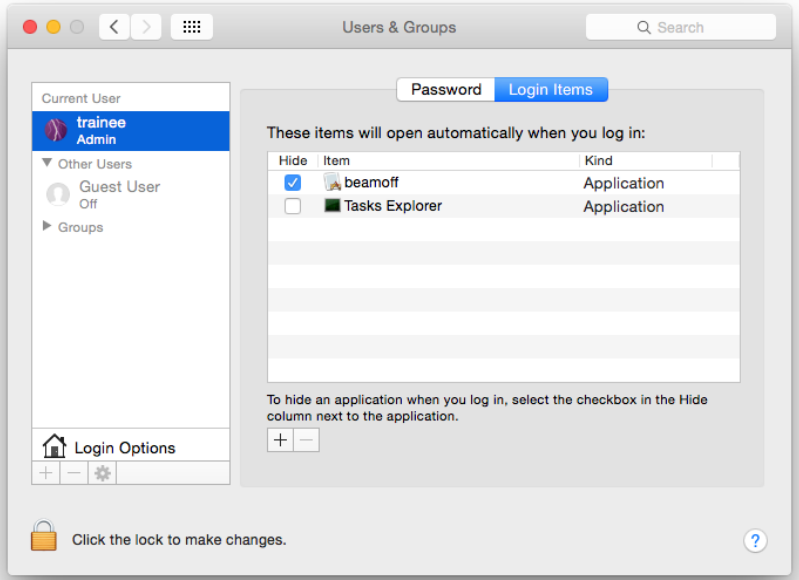
Tools to check for Daemon and Agents

- launchctl
- LaunchControl.app
- Lingon X.app
- lunchy



Login Items

- Associated with a specific user
- SYSTEM PREFERENCES -> USERS & GROUPS -> LOGIN ITEMS
- ~/Library/Preferences/com.apple.loginitems.plist
  - Path is base64 encoding



Re-opening App after Reboot

- On login, any opened windows or apps will be restored
  - Malware could use this as auto-start mechanism
  - ~/Library/Preferences/ByHost/com.apple.loginwindow.<hardware UUID>.plist

Start-up Items

- Automatically executes a script at each reboot
- Place a malicious script and StartUpParameters.plist to:
  - /System/Library/StartupItems
  - /Library/StartupItems

Application Base

- By targeting specific applications logic/framework
  - Plugins and extensions can be used
    - /Users/<user>/Library/Safari/Extensions
    - /Library/Internet Plug-Ins

FileSystem

MAC OS X Filesystem

Scripts
- Perl
- Python
- Bash

Containers
- DMG
- PKG
- Universal Binaries

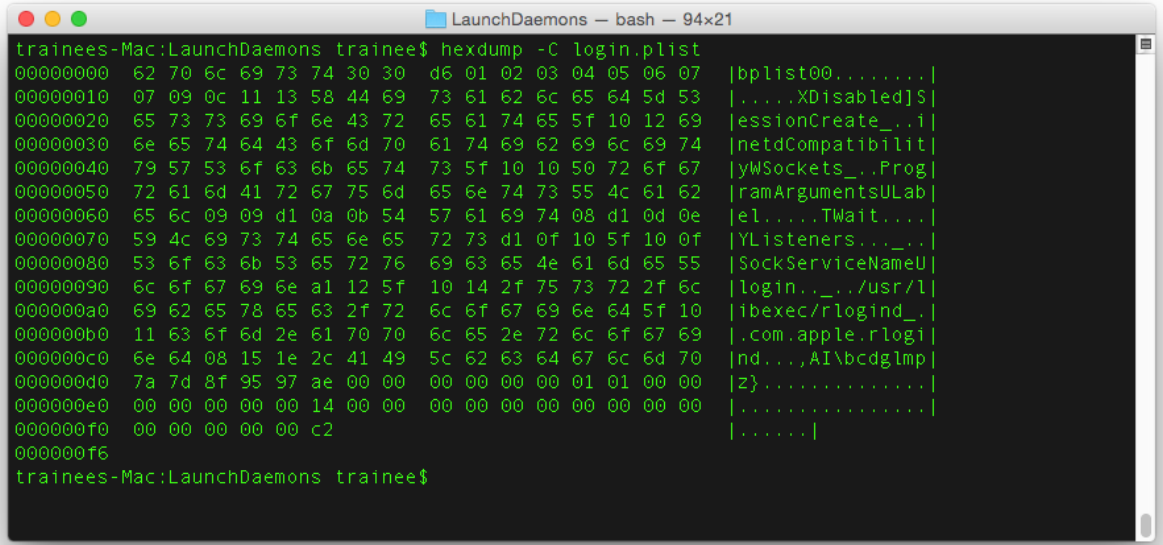
Binaries
- Mach-O (EXE)
- Dylib (DLL)
- Kext (SYS)

Property List

- *.plist
- Settings and configuration
- XML Format
- Like a decentralized registry (windows)

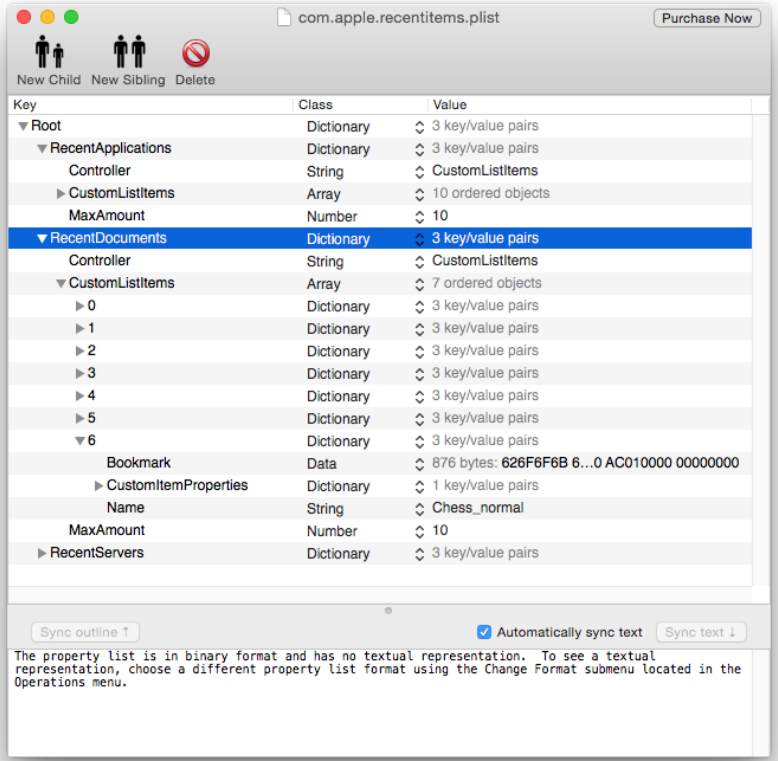
Binary PLIST (complied PLIST)

- One of the several format used by Apple for PLIST
- Signature @ offset 0
  - bplist00
  - bplist01



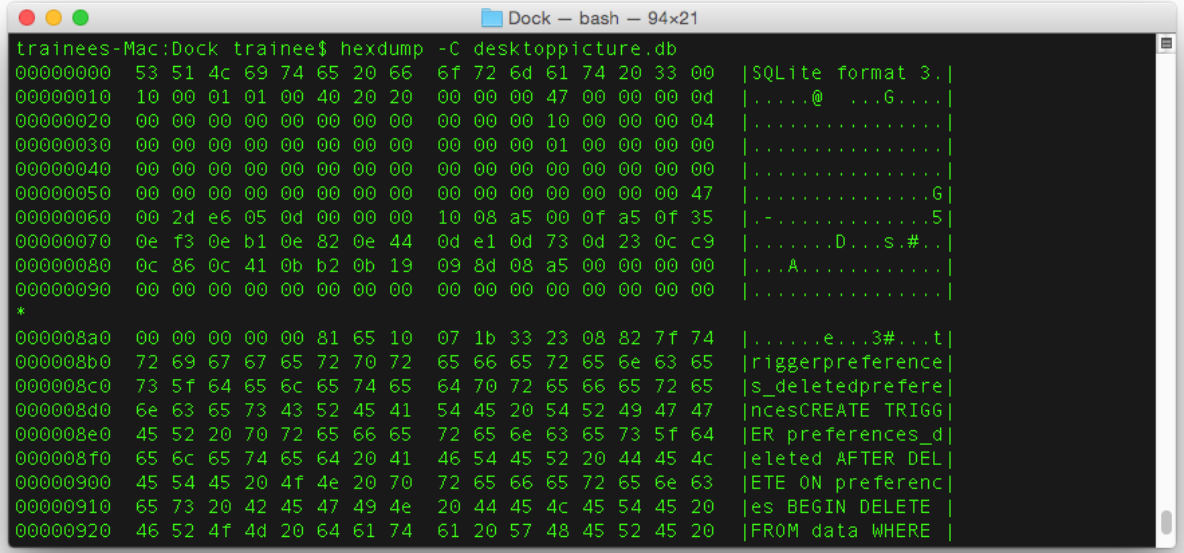
Plist Tools

- Prefs Editor.app
- PlistEdit Pro.app
  - pledit (using command line)
- Pref Setter.app (slow)



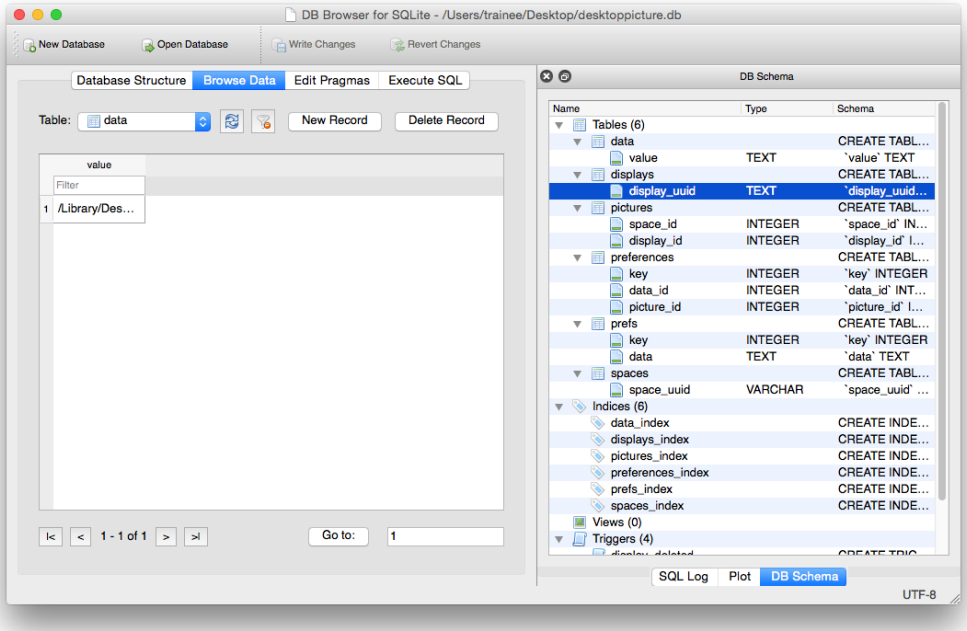
.db files

- Uses SQLite database format
- Signature @ offset 0
  - SQLite



.db Tools

- DB Browser for SQLite
  - http://sqlitebrowser.org/



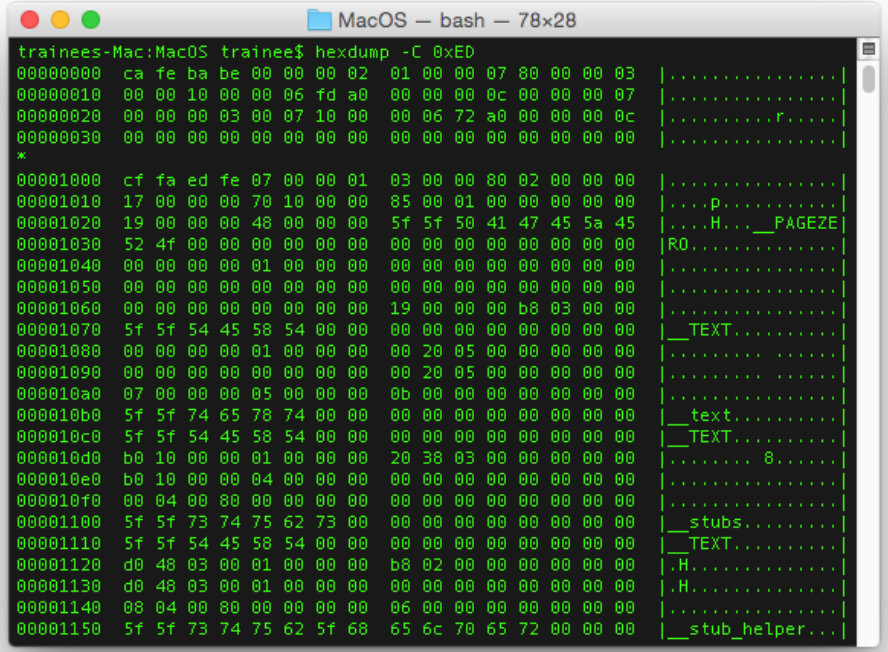
Universal Binaries/Fat Binaries

- Essentially a wrapper – a simple archiver that concatenates Mach-O Files for multiple architectures
- Supports multiple architecture
  - PowerPC
  - Intel 32-bit
  - Intel 64-bit

Fat Binaries

```
struct  at_header {
        uint32_t magic;  “CAFEBABE”
        uint32_t nfat_arch;
};

struct  fat_arch {
        cpu_type_t cputype;
        cpu_subtype_t cpusubtype;
        uint32_t offset;
        uint32_t size;
        uint32_t align;
};
```



Mach-O File Header

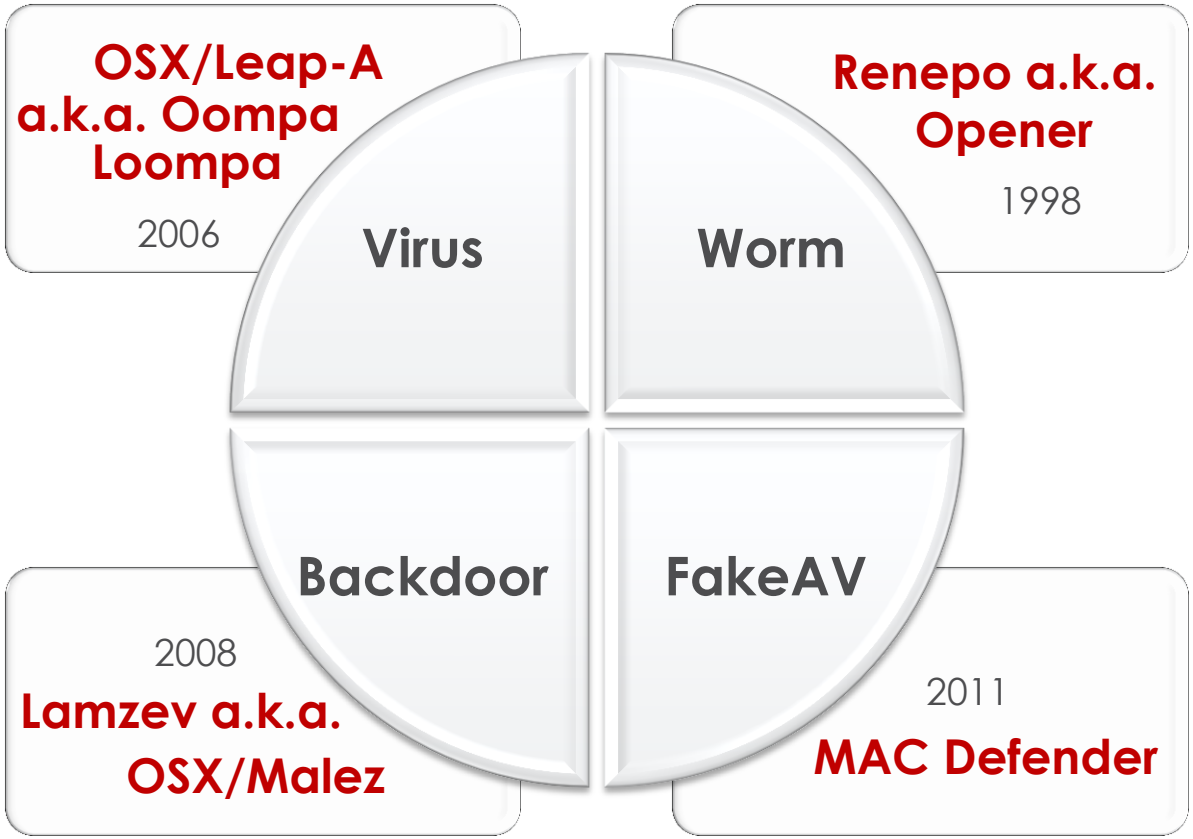
```
struct mach_header {
        uint32_t magic;
        cpu_type_t  cputype;
        cpu_subtype_t cpusubtype;
        uint32_t filetype;
        uint32_t ncmds;
        uint32_t sizeofcmds;
        uint32_t flags;
       uint32_t reserved;   /*available for 64-bit*/
};
```

```
/* Constant for the magic field of the mach_header (32-bit architectures) */
#define MH_MAGIC        0xfeedface      /*POWERPC*/
#define MH_CIGAM        0xcefaedfe      /*Intel*/

/* Constant for the magic field of the mach_header_64 (64-bit
architectures) */
#define MH_MAGIC_64 0xfeedfacf      /* POWERPC*/
#define MH_CIGAM_64 0xcffaedfe      /*Intel*/
```

MAC Malware Trends

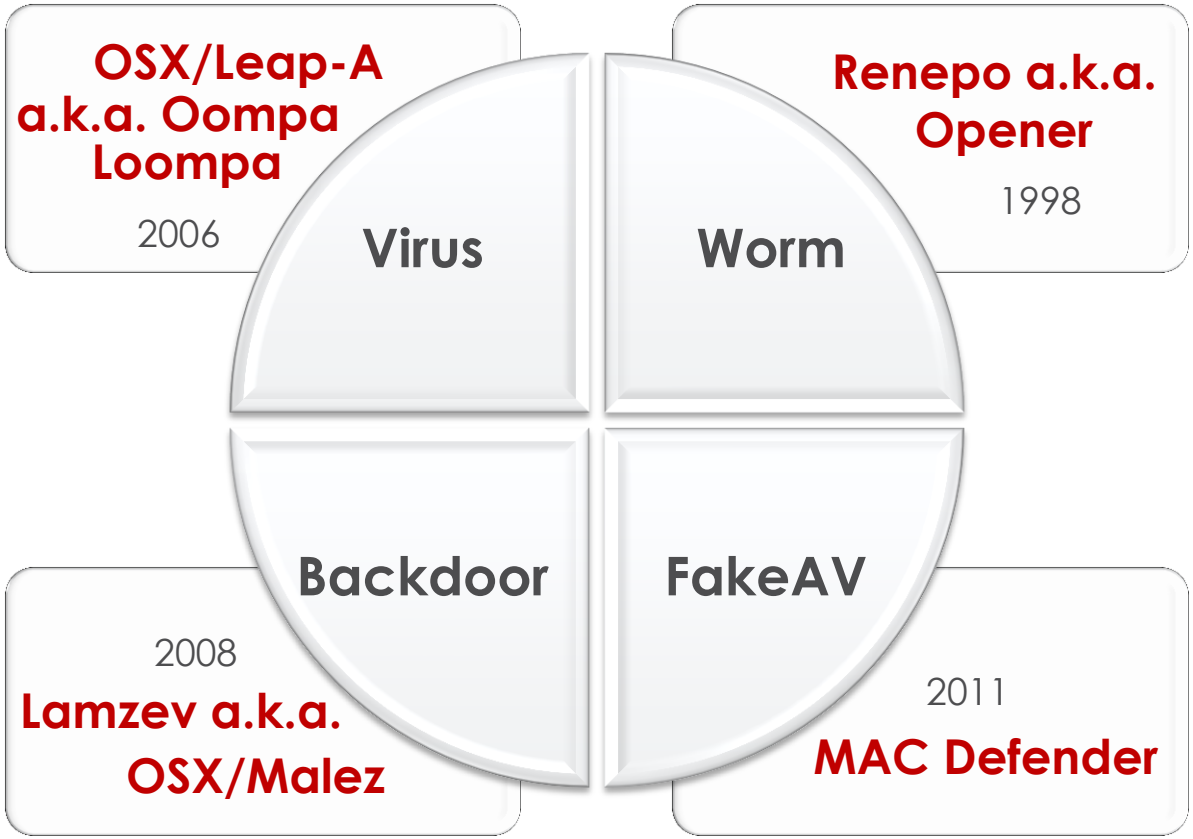
First MAC Malwares



OSX/Leap-A a.k.a. Oompa Loompa

- disguised as simple image file
- infects Cocoa applications
- spread via iChat instant messaging

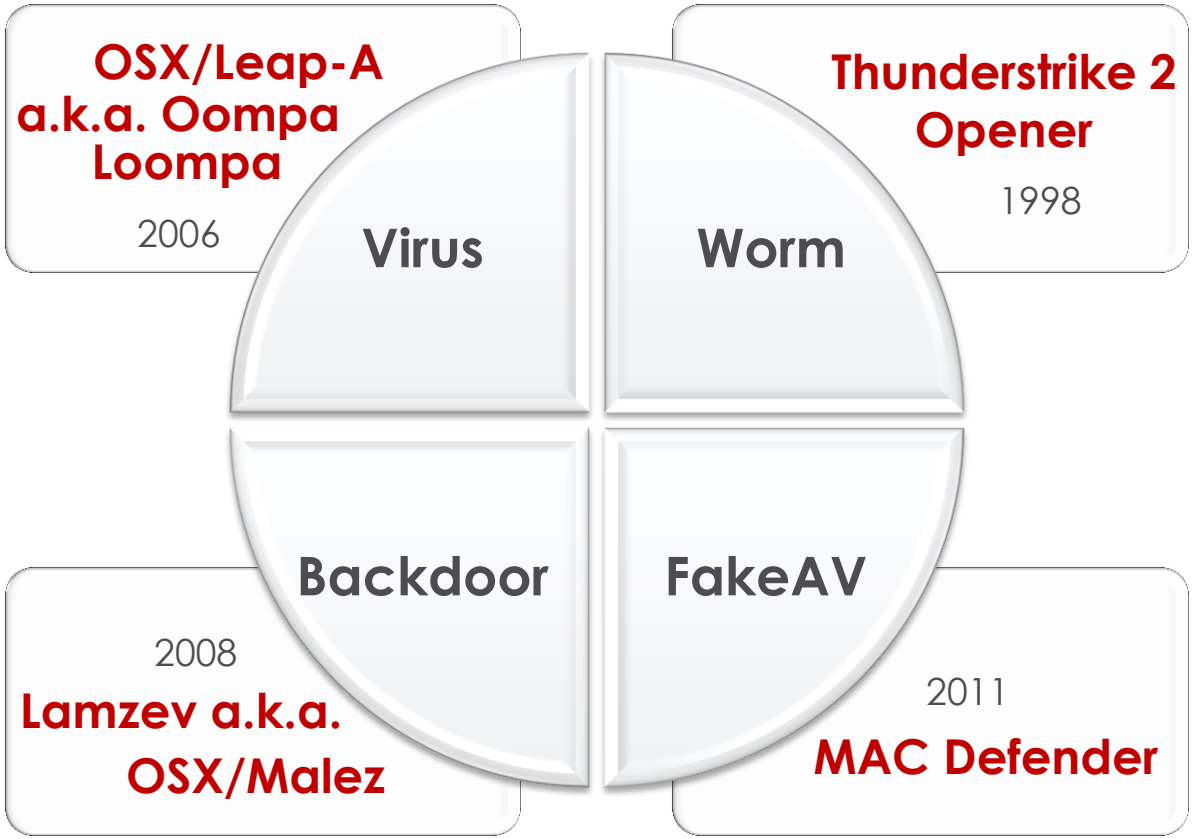
First MAC Malwares



Renepo a.k.a. Opener

- self-propagating worm by gaining root access
- propagates via networks and drives
- turns off OS X firewall

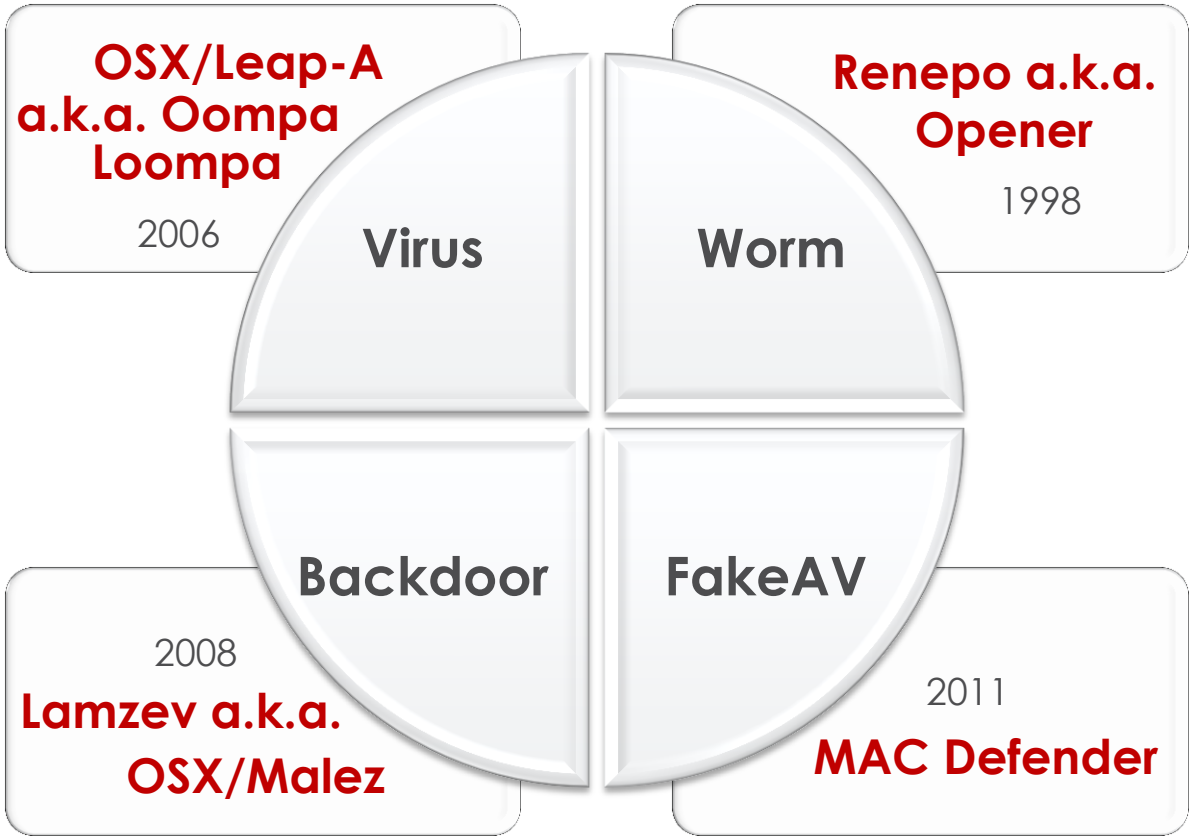
First MAC Malwares



Lamzev a.k.a. OSX/Malez

- hacker tool to install backdoor
- needs physical access to the system

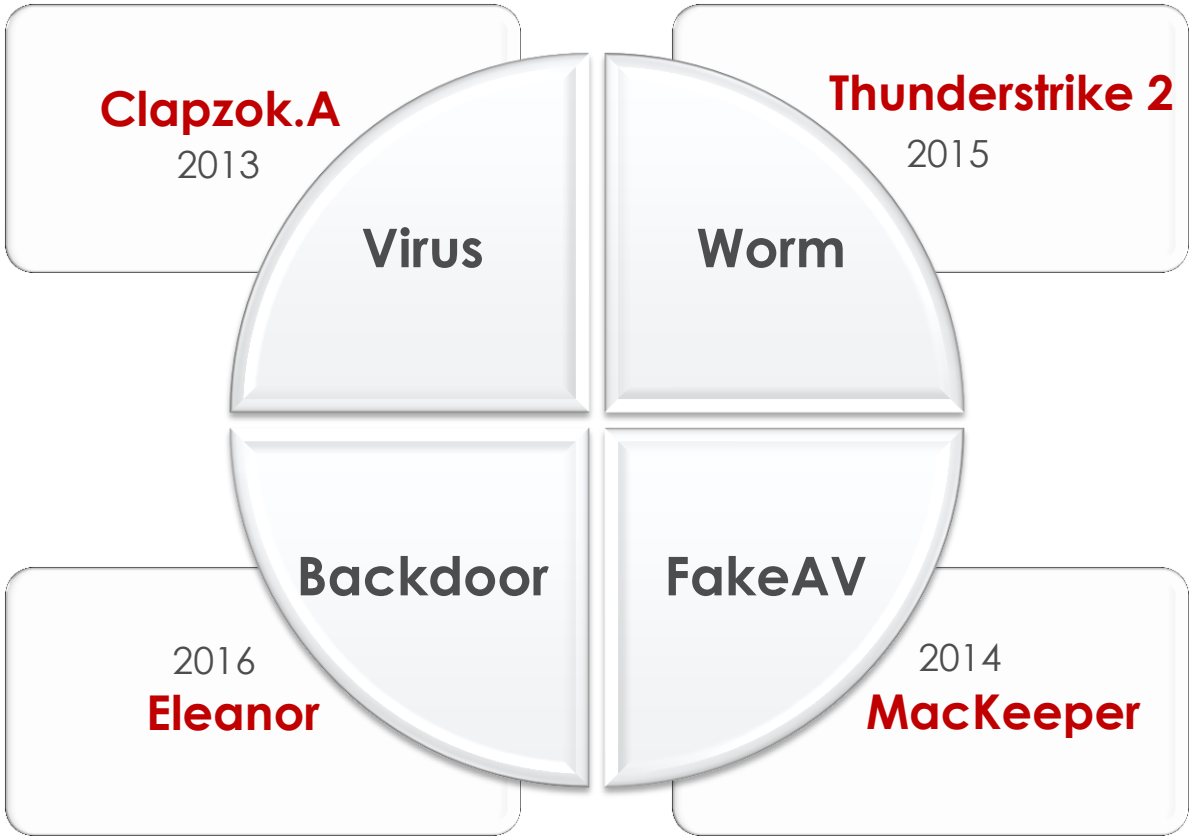
First MAC Malwares



MAC Defender

- attack similar to ones on Windows
- took the name of legitimate MacDefender program
- poisoned popular search terms

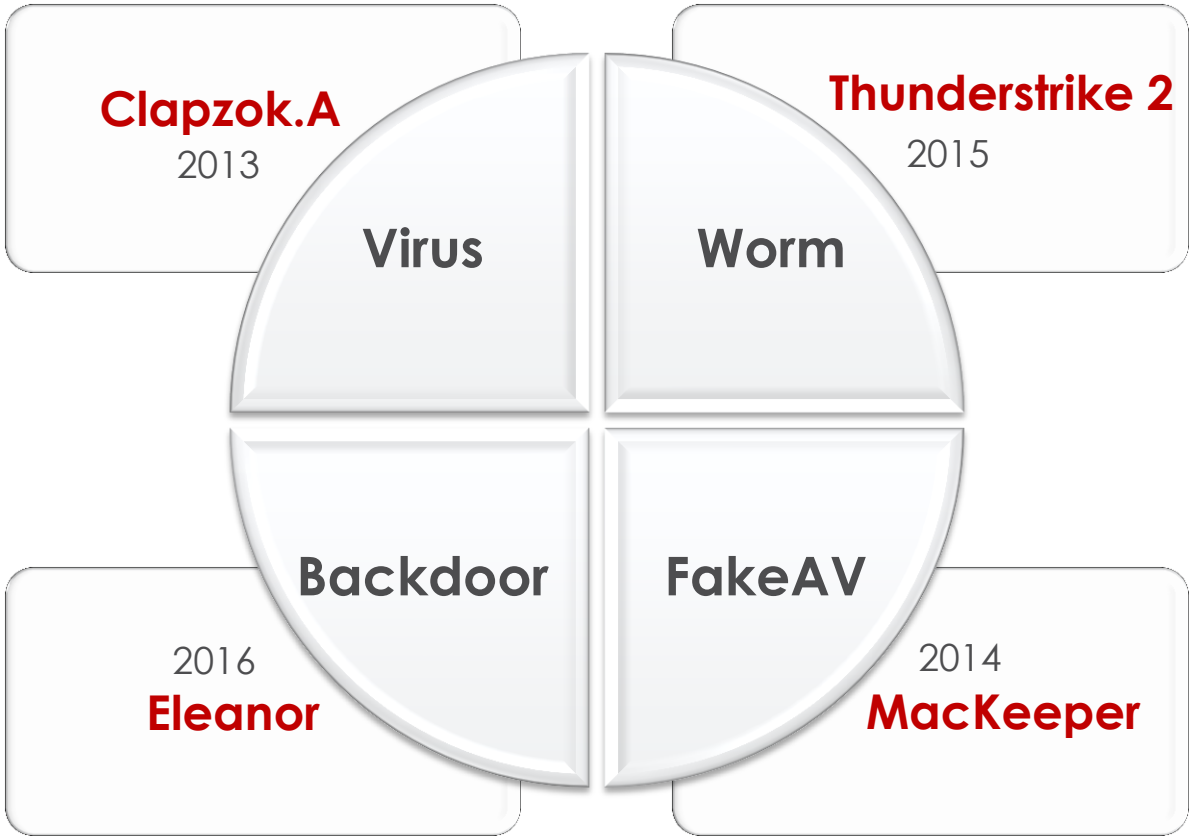
More Recent MAC Malwares



Clapzok.A

- proof-of-concept virus by JPanic, updated version of a Windows virus
- only infects x86 versions
- multi-platform infection

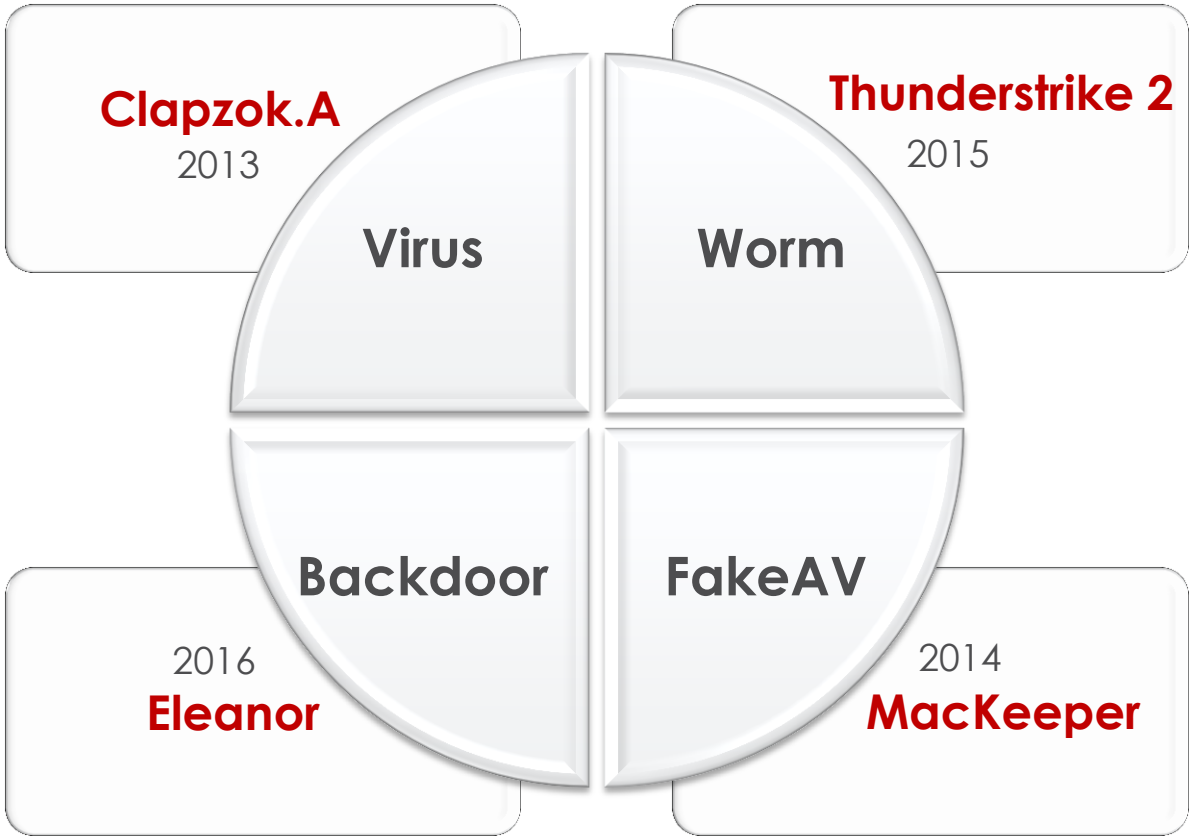
More Recent MAC Malwares



Thunderstrike 2

- proof-of-concept worm by security researchers
- stealth firmware worm
- can spread once option ROM on peripheral devices is infected

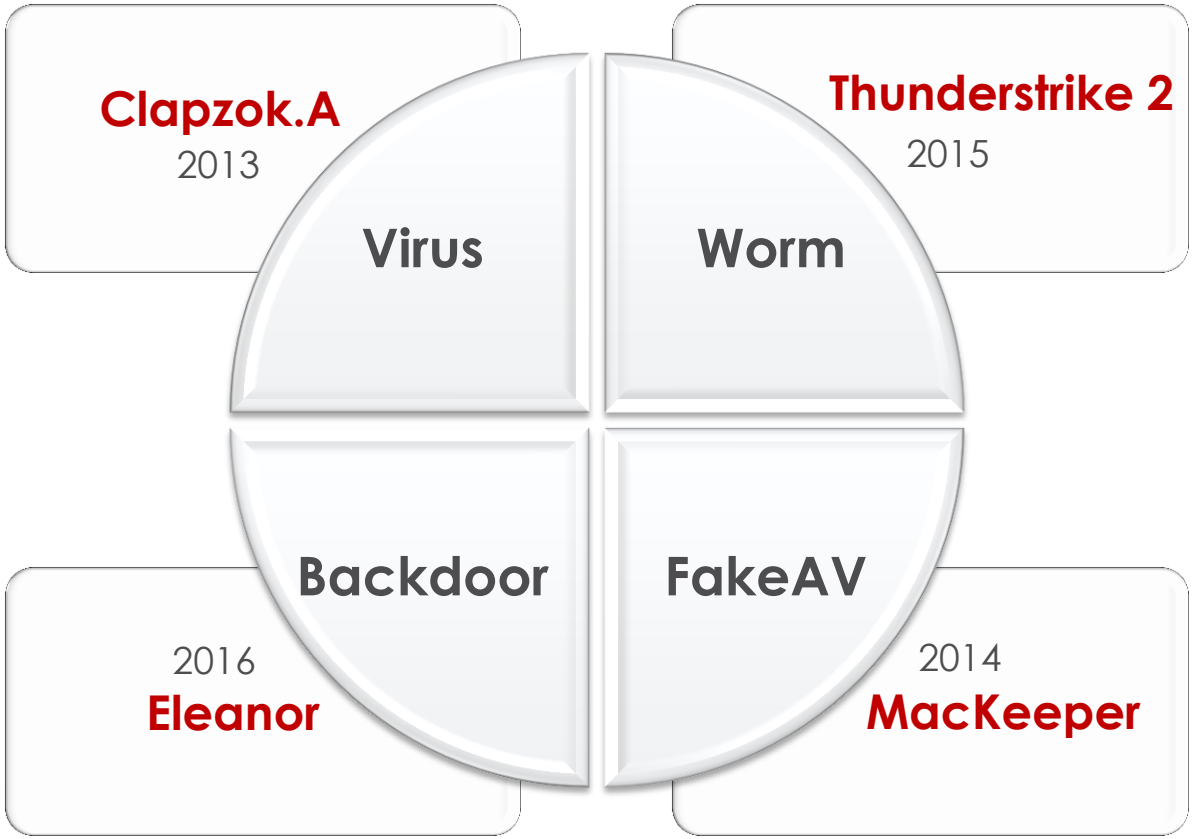
More Recent MAC Malwares



Eleanor

- distributed as Easydoc Converter
- connects infected PC to TOR network and generates .onion domain to access user's system using only the browser

More Recent MAC Malwares



MacKeeper

- utility software for "MAC OS X security and optimization"

MAC Ransomware: KeRanger

Transmission v2.90
dmg installer

General.rtf

UPX-packed
Mach-O
Executable

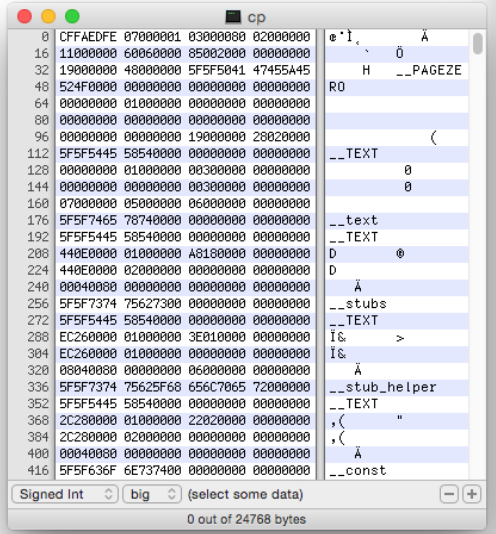
kernel_pid;
kernel_time;
kernel_complete

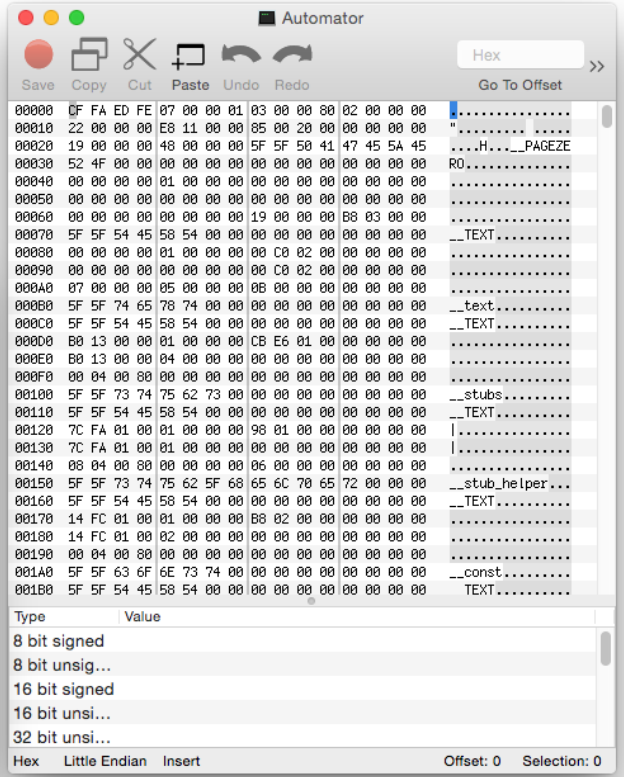
encrypts users' files
and hold these for
ransom

Tools For Static Analysis

HexDumpers

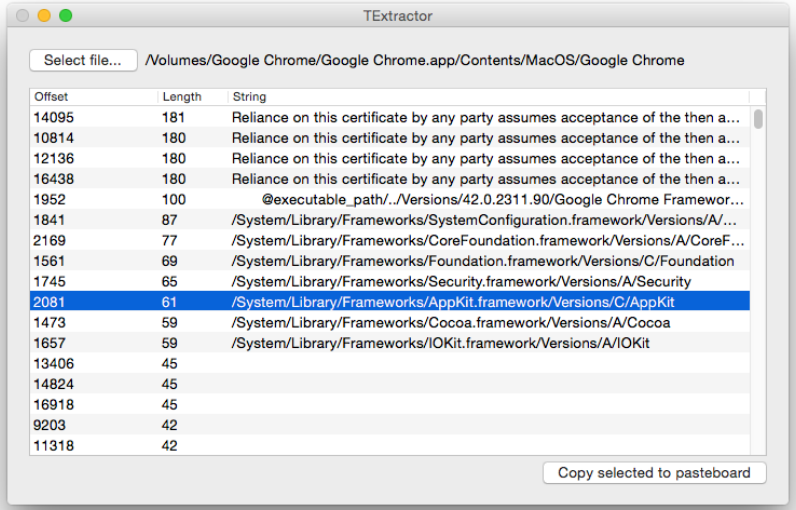
- Display a hexdump of a binary file
  - hexdump –C <filename>
  - OxED.app (GUI)
  - Hex Fiend (GUI)





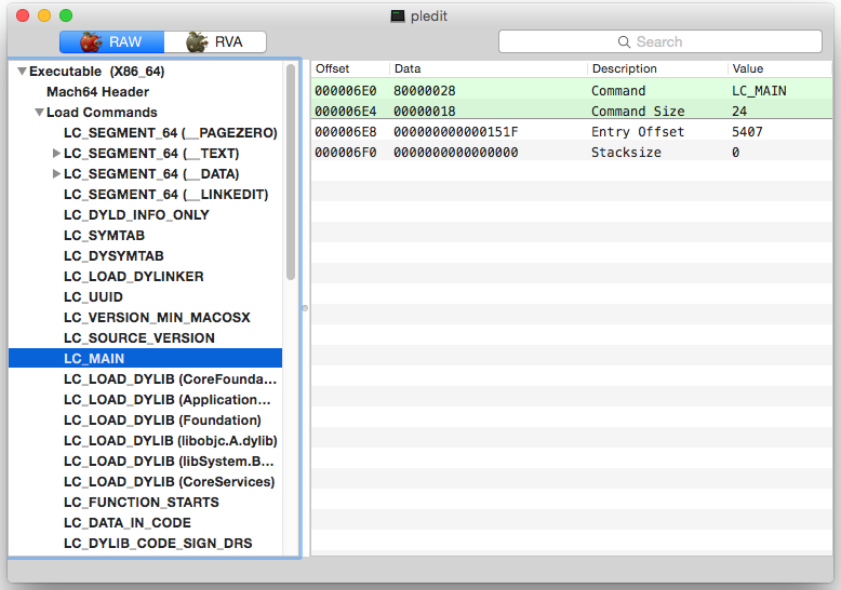
File String Extraction

- Search for a pattern
  - grep ‘regex pattern’ <filename>
- Search for strings
  - strings <filename>
- String extractor
  - TExtractor.app (GUI)



Mach-O File Analysis Tools

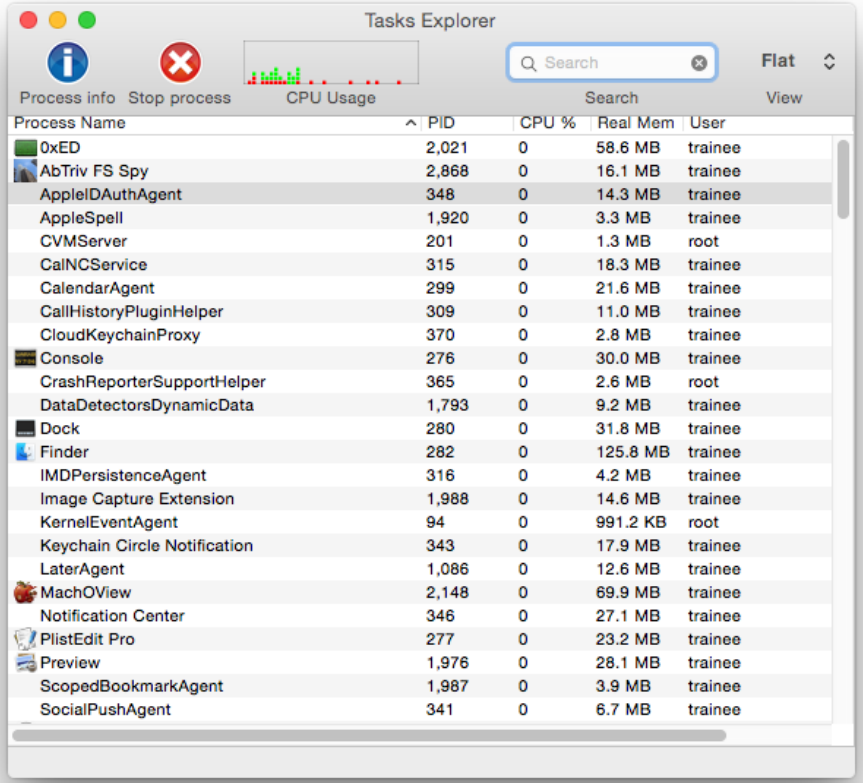
- Displays and parse the whole Mach-O file
  - MachOView.app (GUI)
  - Otool
  - **machoviz**.anrc-services.com



Tools For Dynamic Analysis

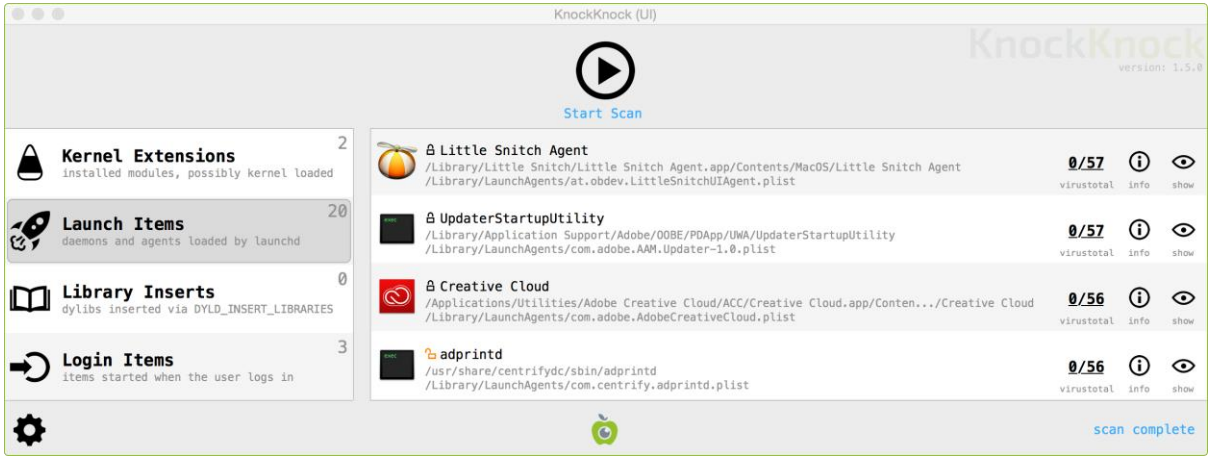
Process Monitoring

- Display running processes
  - Activity Monitor.app (GUI)
  - Task Explorer.app (GUI)
  - top | grep ‘process name’
  - ps -ef | grep ‘process name’



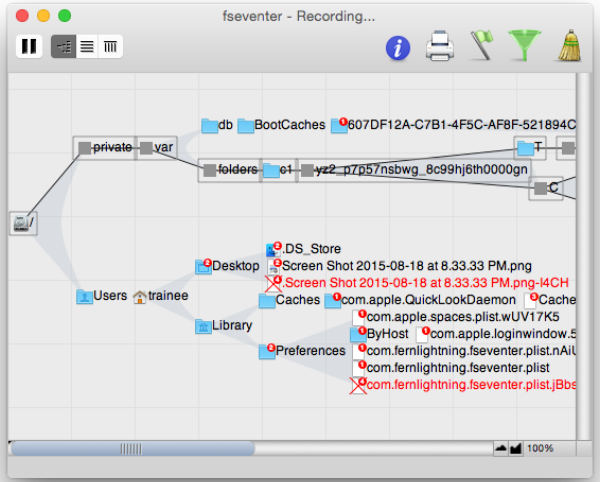
Persistence Monitoring

- Display lauch daemons or agents
  - lauchctl list
  - KnockKnock



FileSystem Monitoring

- Watch filesystem in realtime in console
  - fs_usage
- Graphical view of filesystem events
  - fseventer.app (GUI)
- Track file system activity
  - AbTriv FS Spy.app (GUI)
- List open files
  - lsof

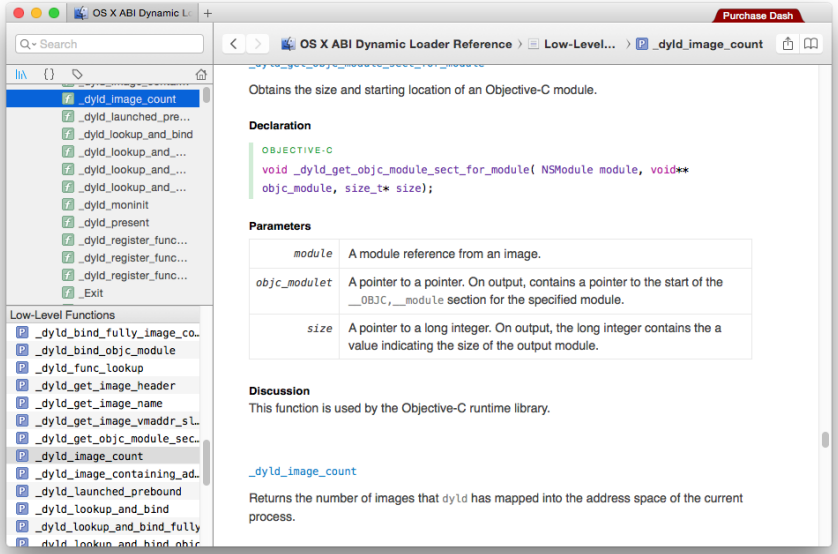


Network Monitoring

- Network Traffic Analysis
  - Wireshark.app (GUI)
- HTTP Parser
  - Fetcher.app (GUI)
- List active network connections
  - PortsMonitor.app (GUI)
  - netstat –a

Other Tools

- Text and Source Code Editors
  - TextWrangler.app
  - Tincta.app
- API Documentation Browser
  - Dash.app



Conclusion

Learn MAC Malware Analysis NOW!

References:

- Jonathan Levin: MAC OS X and iOS Internals
- http://electronics.howstuffworks.com/tech-myths/5-myths-about-apple10.htm
- https://www.rsaconference.com/writable/presentations/file_upload/ht-r03-malware-persistence-on-os-x-yosemite_final.pdf
- https://objective-see.com/products/knockknock.html

References:

- http://www.toptenreviews.com/software/articles/history-of-macintosh-viruses/
- https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/

VIRUS

- http://www.macworld.com/article/1049459/leapafaq.html
- http://reverse.put.as/2013/05/31/clapzok-a-reversing-the-os-x-part-of-a-multiplatform-poc-infector/

WORM

- https://www.macobserver.com/tmo/article/Renepo_Worm_Targets_Mac_OS_X
- https://www.wired.com/2015/08/researchers-create-first-firmware-worm-attacks-macs/

BACKDOOR

- http://www.zdnet.com/article/mac-os-x-targeted-by-trojan-and-backdoor-tool/
- http://news.softpedia.com/news/new-malware-uses-tor-to-open-backdoor-on-mac-os-x-systems-506000.shtml

FAKEAV

- http://www.eweek.com/c/a/Security/Fake-AV-Targets-Mac-OS-X-Through-Poisoned-Search-Links-644121
- http://www.thesafemac.com/ongoing-mackeeper-fraud/
- https://discussions.apple.com/docs/DOC-3036

RANSOMWARE

- http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

macOS Sierra

- http://www.macrumors.com/roundup/macos-sierra/

Thank you!!!