



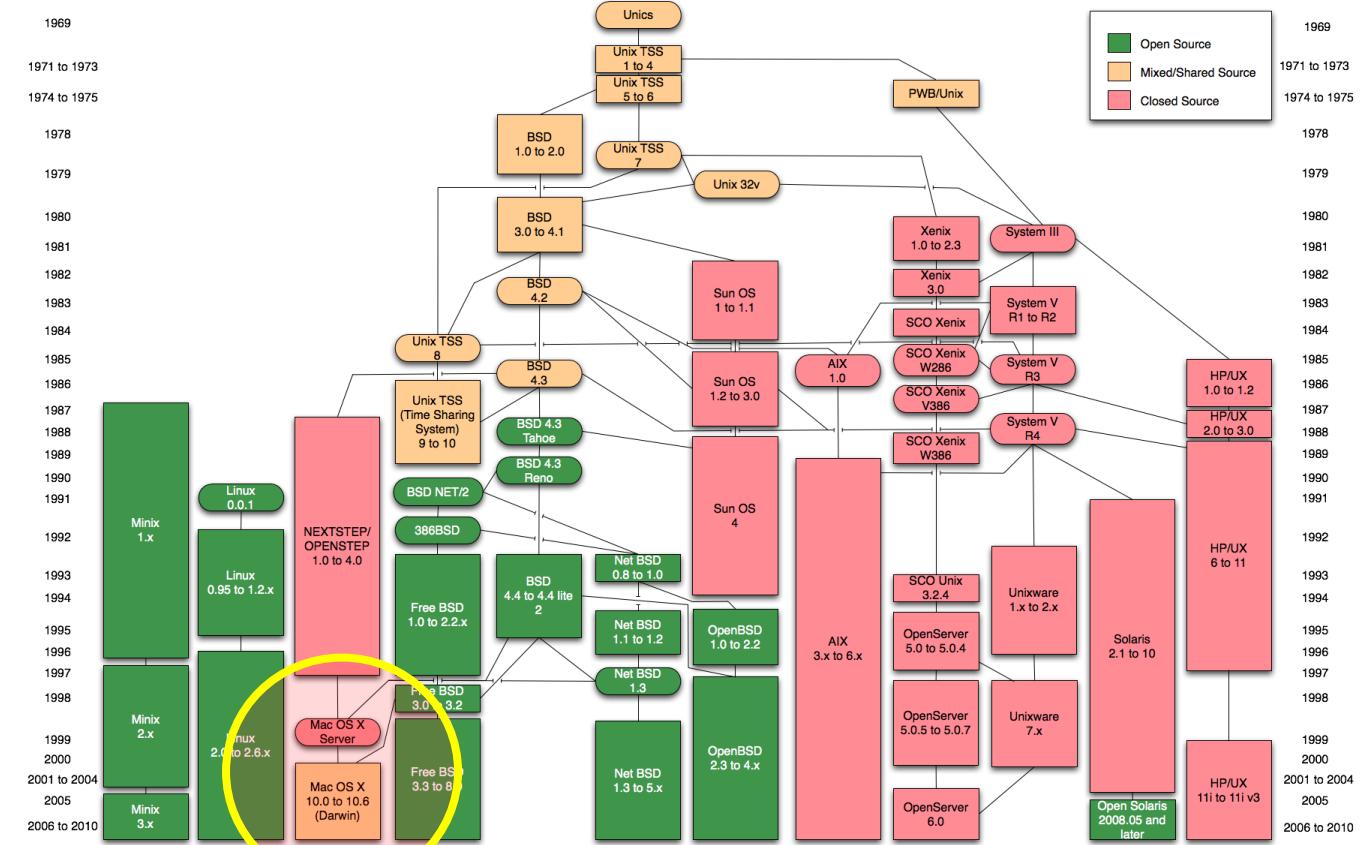
Shifting Paradigms from Windows to Mac

Nicholas Ramos and Michelle Morales



Introduction to MAC OS X

Review



MAC OS X Timeline

2009	10.6 – Snow Leopard
2011	10.7 - Lion
2012	10.8 – Mountain Lion
2013	10.9 - Mavericks
2014	10.10 - Yosemite
2015	10.11 – El Capitan
2016	10.12 – macOS Sierra

Getting to Know More

MAC vs. Windows



*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

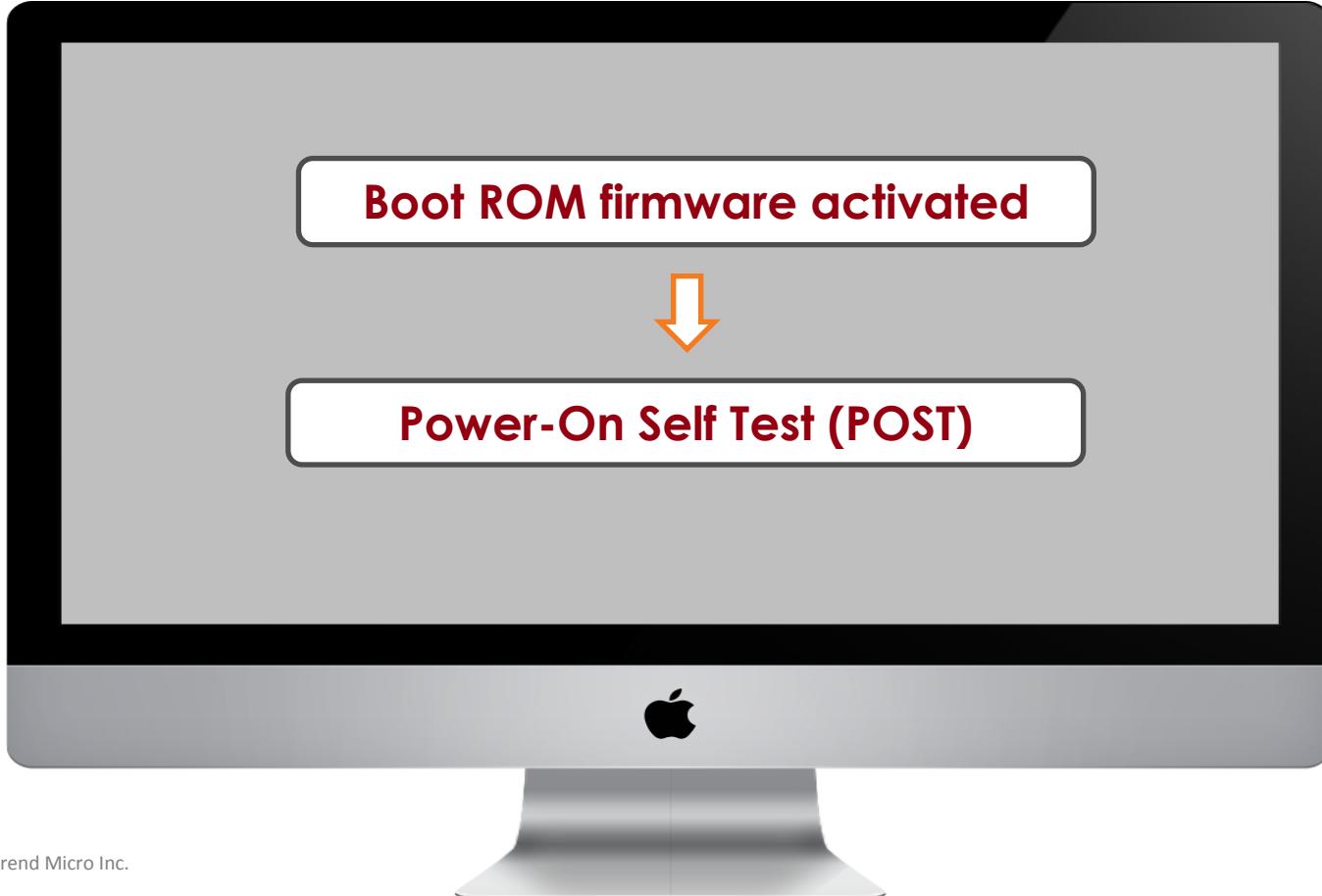
- Only signed kext (drivers) can be loaded

OS X Boot-up Process

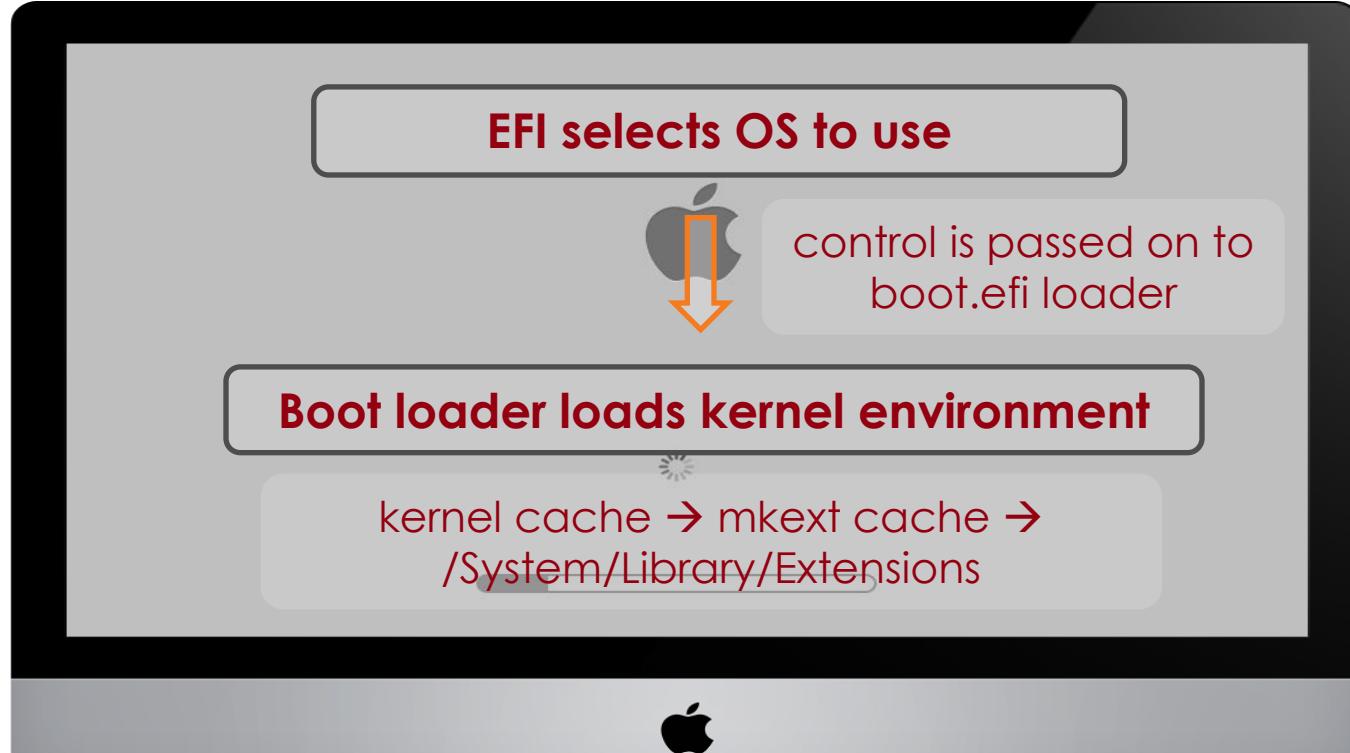
MAC Boot-Up



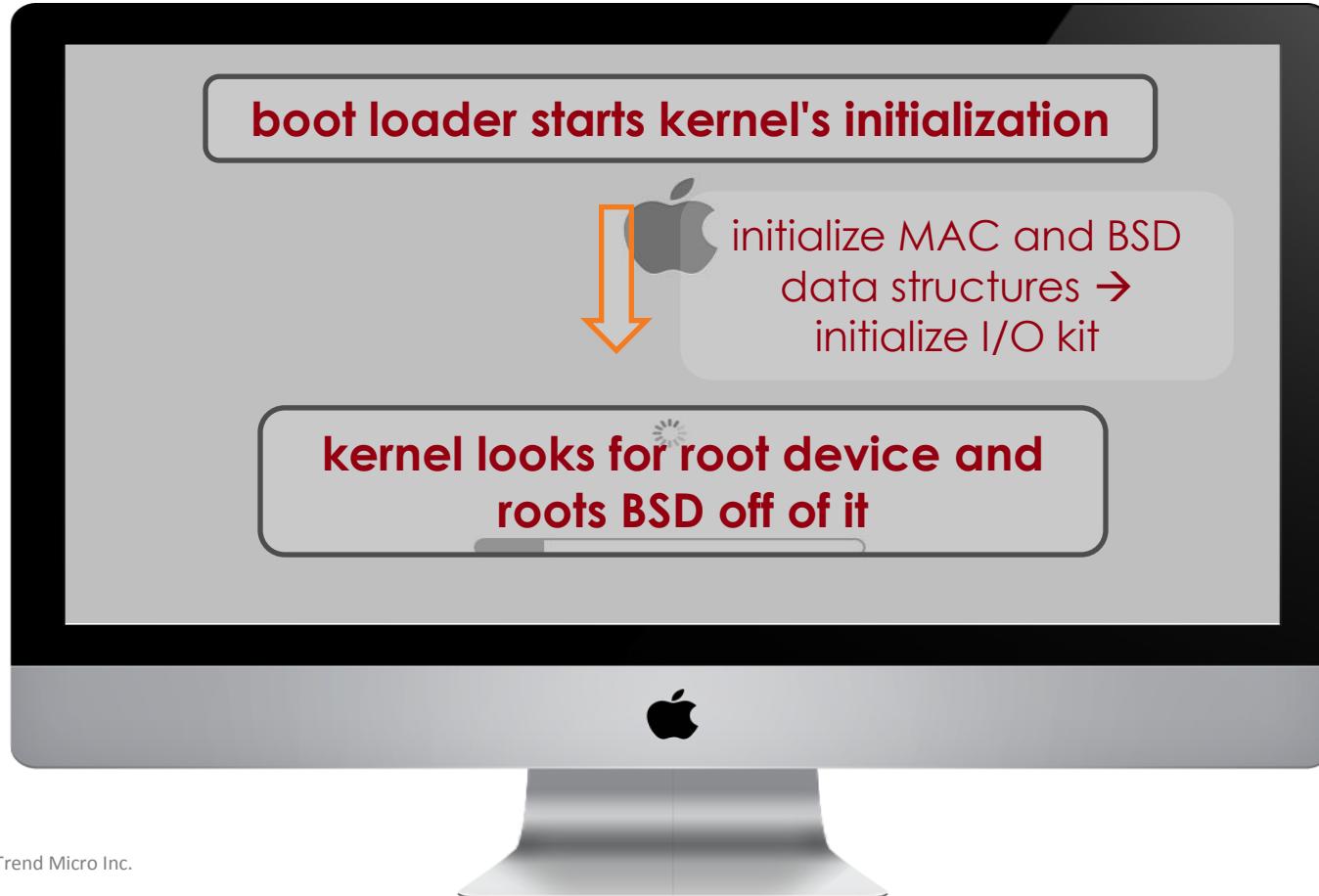
MAC Boot-Up



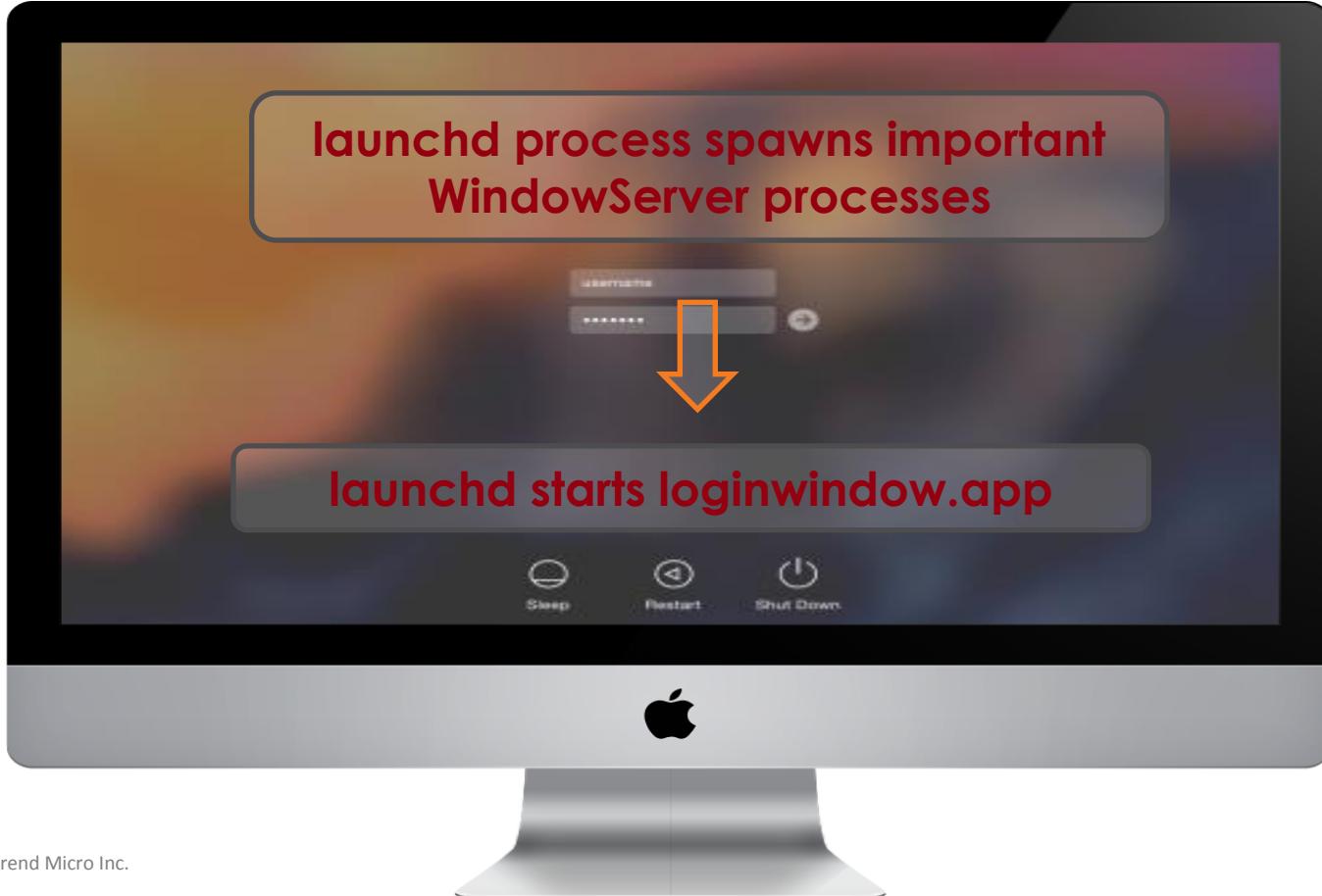
MAC Boot-Up



MAC Boot-Up



MAC Boot-Up



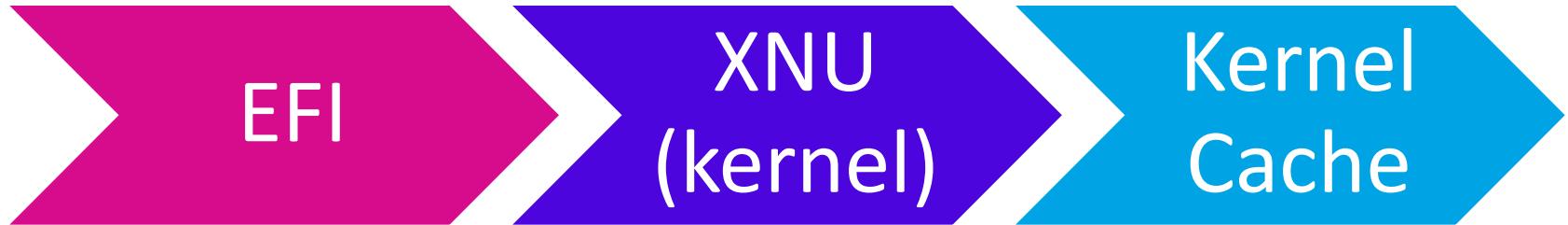
MAC Boot-Up



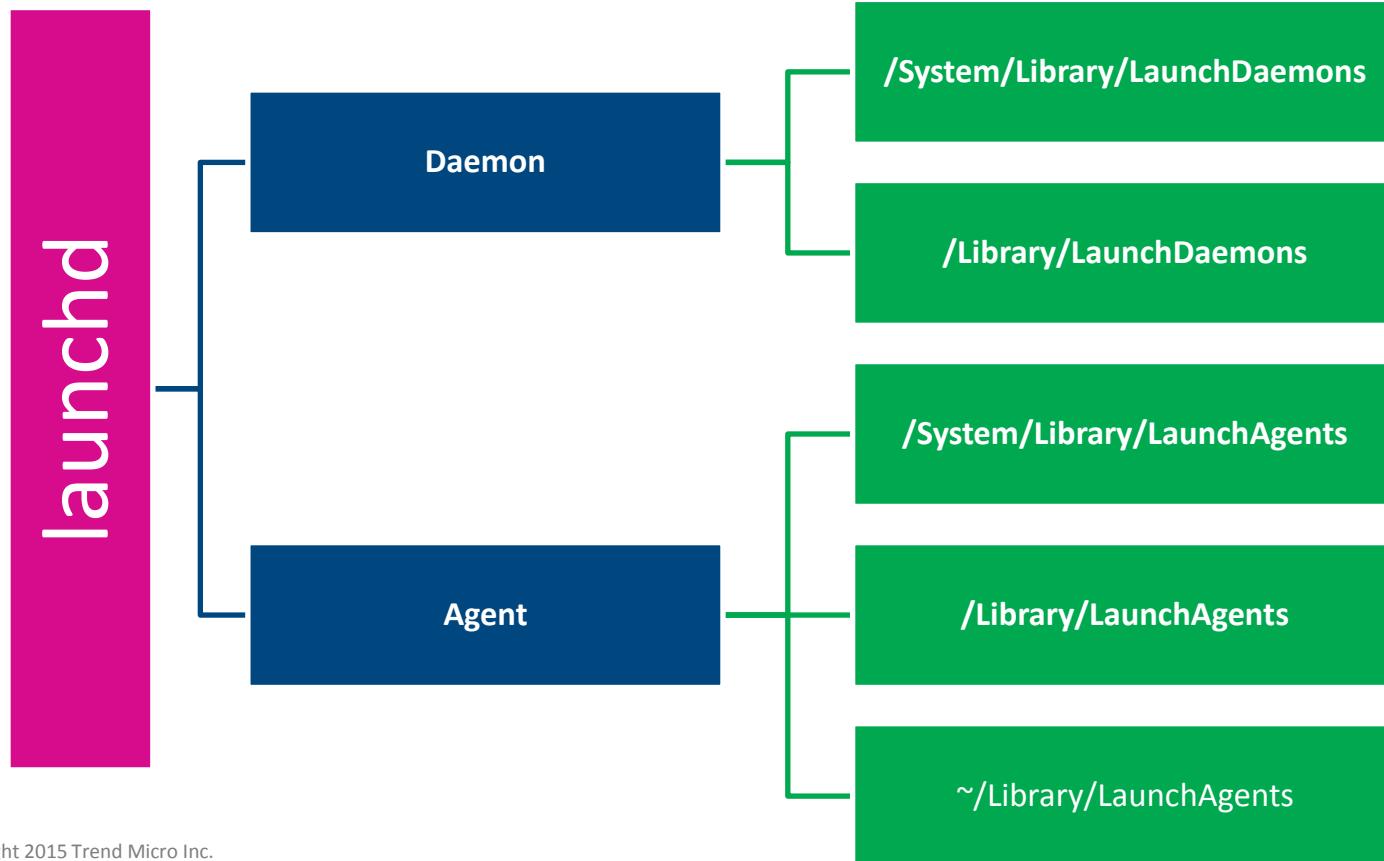
Auto-Start Mechanism

TRICKS AND WAYS FOR MALWARE PERSISTENCE

Pre-Login Persistence



Launched as Daemon or Agent

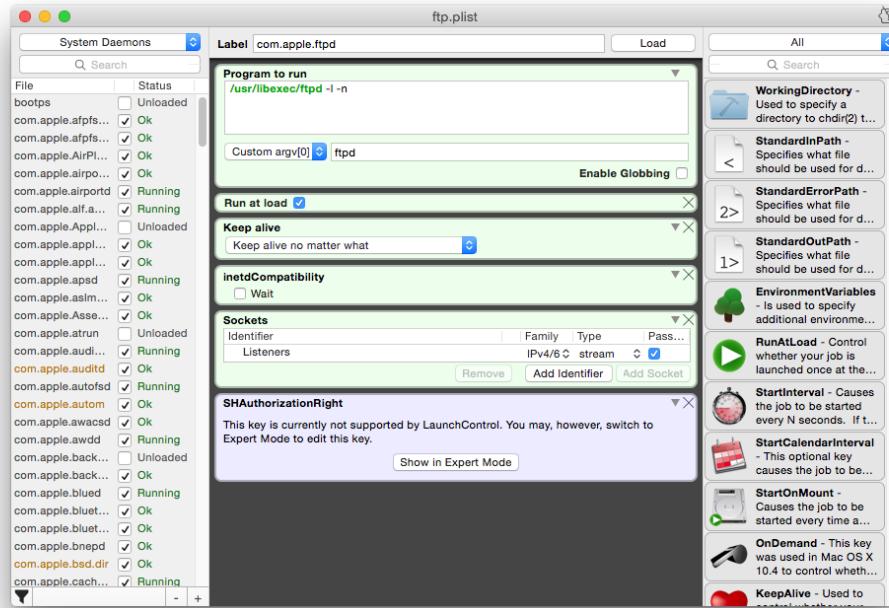


Type of Launched Daemons and Agents

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

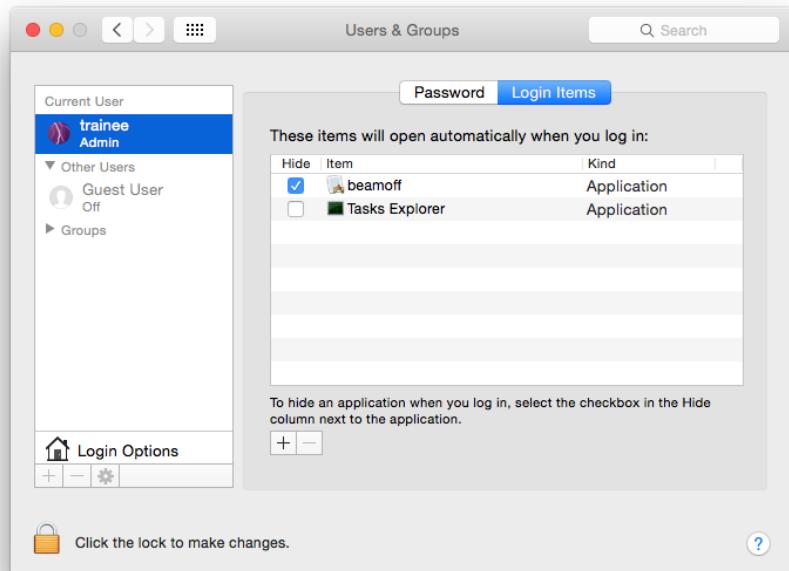
Tools to check for Daemon and Agents

- 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

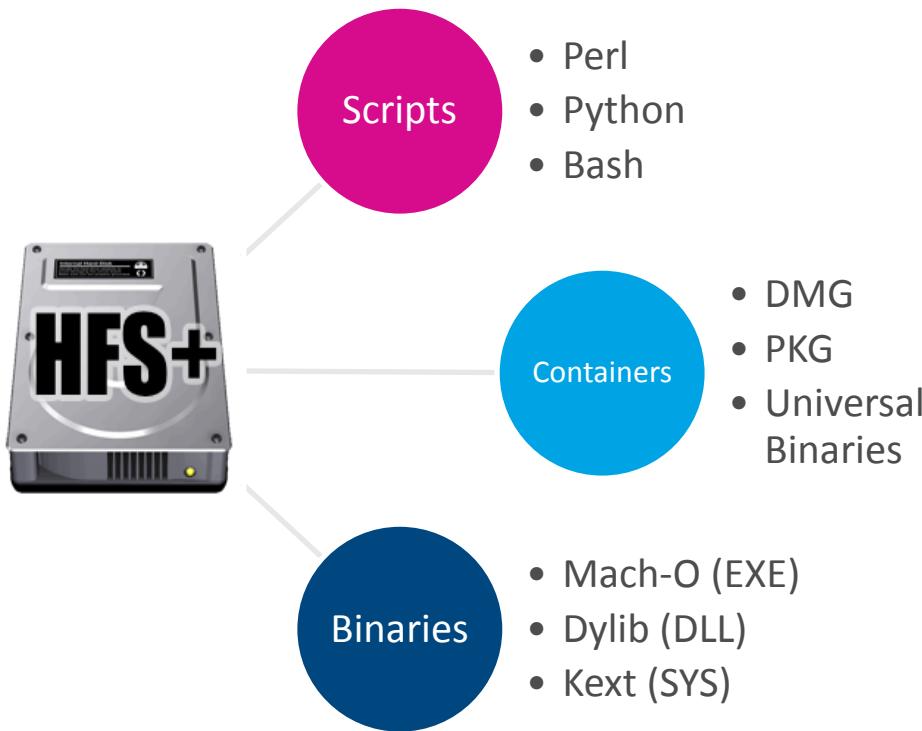
- Automatically executes a script at each reboot
- Place a malicious script and StartUpParameters.plist to:
 - /System/Library/StartupItems
 - /Library/StartupItems

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



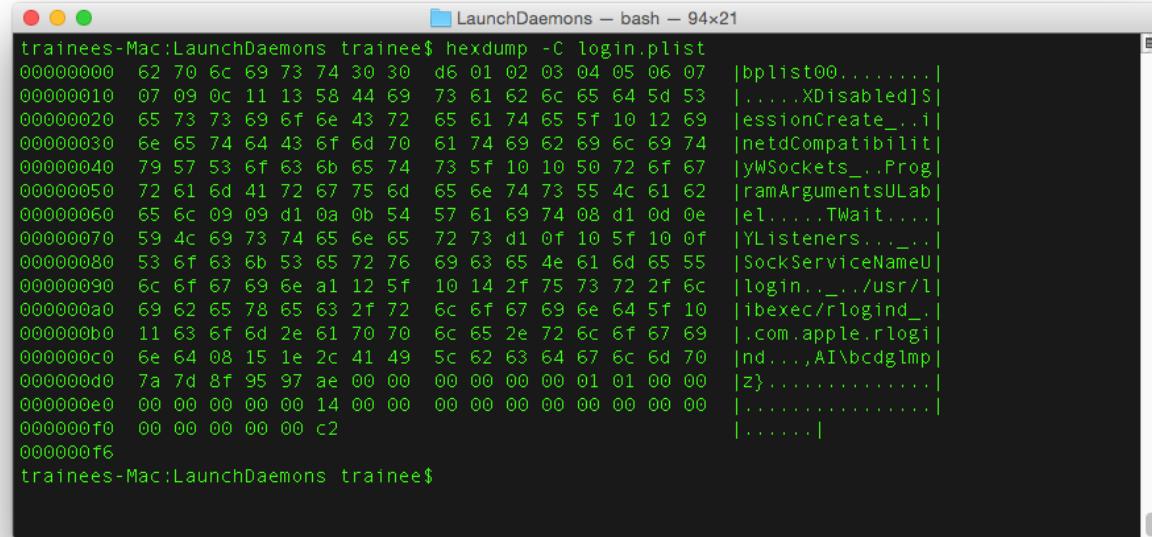
Property List

- *.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

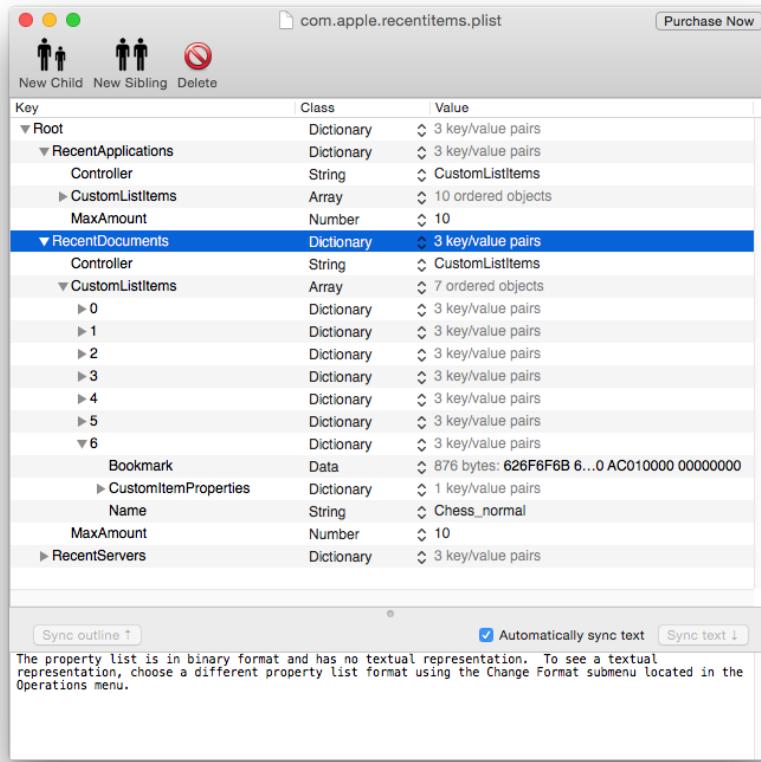


The screenshot shows a terminal window titled "LaunchDaemons - bash - 94x21". The command "hexdump -C login.plist" is run, displaying the raw hex and ASCII representation of the file. The ASCII output reveals parts of the XML plist structure, including keys like "bplist00", "XDisabled", "sessionCreate_..i", "netdCompatibilit", "yWSockets_..Prog", "ramArgumentsULab", "el....TWait....", "YListeners..._..", "SockServiceNameU", "login.../usr/l", ".ibexec/flogind_..", ".com.apple.rlogin", "nd...,AI\bcdglmp", "z>.....", and ".....". The terminal prompt "trainees-Mac:LaunchDaemons trainee\$" is visible at the bottom.

```
trainees-Mac:LaunchDaemons trainee$ hexdump -C login.plist
00000000  62 70 6c 69 73 74 30 30  d6 01 02 03 04 05 06 07  |bplist00.....|
00000010  07 09 0c 11 13 58 44 69  73 61 62 6c 65 64 5d 53  |.....XDisabled]S|
00000020  65 73 73 69 6f 6e 43 72  65 61 74 65 5f 10 12 69  |sessionCreate_.i|
00000030  6e 65 74 64 43 6f 6d 70  61 74 69 62 69 6c 69 74  |netdCompatibilit|
00000040  79 57 53 6f 63 6b 65 74  73 5f 10 10 50 72 6f 67  |yWSockets_..Prog|
00000050  72 61 6d 41 72 67 75 6d  65 6e 74 73 55 4c 61 62  |ramArgumentsULab|
00000060  65 6c 09 09 d1 0a 0b 54  57 61 69 74 08 d1 0d 0e  |el....TWait....|
00000070  59 4c 69 73 74 65 6e 65  72 73 d1 0f 10 5f 10 0f  |YListeners..._..|
00000080  53 6f 63 6b 53 65 72 76  69 63 65 4e 61 6d 65 55  |SockServiceNameU|
00000090  6c 6f 67 69 6e a1 12 5f  10 14 2f 75 73 72 2f 6c  |login.../usr/l|
000000a0  69 62 65 78 65 63 2f 72  6c 6f 67 69 6e 64 5f 10  |.ibexec/flogind_..|
000000b0  11 63 6f 6d 2e 61 70 70  6c 65 2e 72 6c 6f 67 69  |.com.apple.rlogin|
000000c0  6e 64 08 15 1e 2c 41 49  5c 62 63 64 67 6c 6d 70  |nd...,AI\bcdglmp|
000000d0  7a 7d 8f 95 97 ae 00 00  00 00 00 00 01 01 00 00  |z>.....|
000000e0  00 00 00 00 00 14 00 00  00 00 00 00 00 00 00 00 00  |.....|
000000f0  00 00 00 00 00 c2 00 00  |.....|
00000100
```

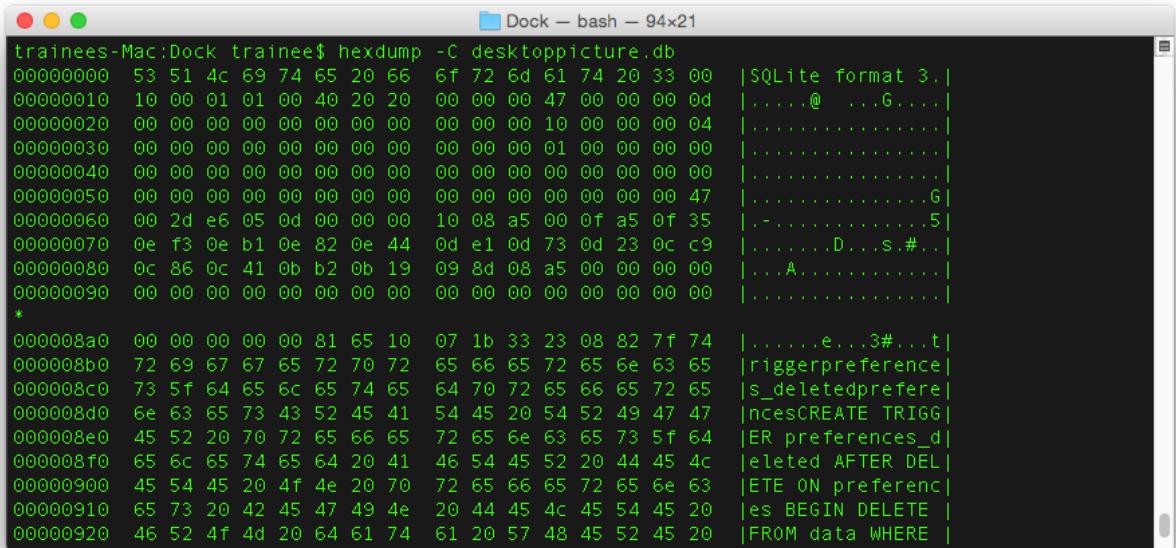
Plist Tools

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



.db files

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

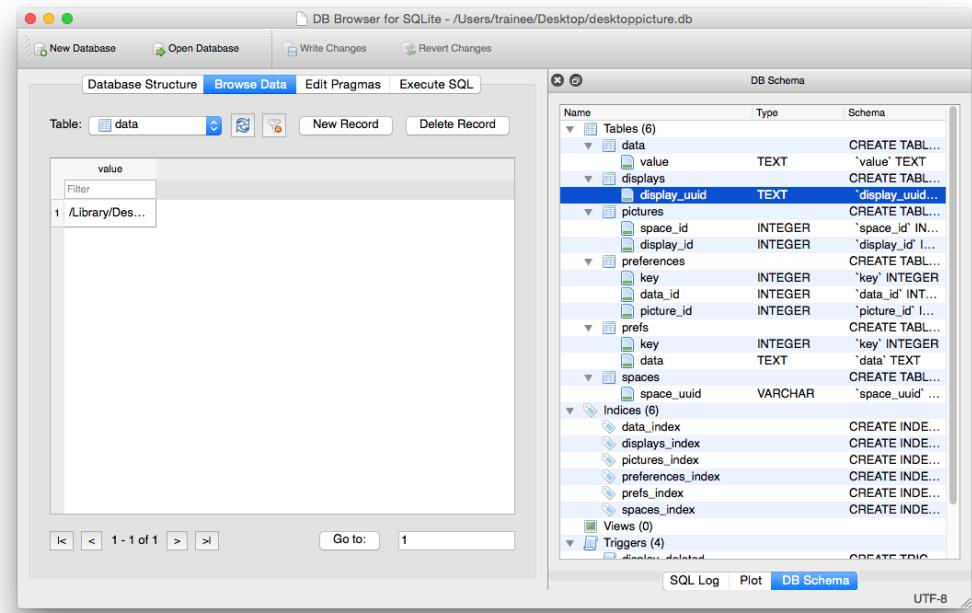


The screenshot shows a terminal window titled "Dock – bash – 94x21". The command entered is "trainees-Mac:Dock trainee\$ hexdump -C desktoppicture.db". The output displays the raw hex and ASCII data of the SQLite database file. The ASCII output includes recognizable SQL commands like "CREATE TABLE", "INSERT INTO", and "SELECT" statements, along with other database metadata and data rows.

```
trainees-Mac:Dock trainee$ hexdump -C desktoppicture.db
00000000  53 51 4c 69 74 65 20 66  6f 72 6d 61 74 20 33 00 |SQLite format 3.| 
00000010  10 00 01 01 00 40 20 20  00 00 00 47 00 00 00 0d |.....@ ...G....| 
00000020  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 04 |.....| 
00000030  00 00 00 00 00 00 00 00  00 00 00 01 00 00 00 00 |.....| 
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |.....| 
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 47 |.....G| 
00000060  00 2d e6 05 0d 00 00 00  10 08 a5 00 0f a5 0f 35 |.....5| 
00000070  0e f3 0e b1 0e 82 0e 44  0d e1 0d 73 0d 23 0c c9 |.....D...S.#..| 
00000080  0c 86 0c 41 0b b2 0b 19  09 8d 08 a5 00 00 00 00 |...A.....| 
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |.....| 
*
0000008a0  00 00 00 00 00 81 65 10  07 1b 33 23 08 82 7f 74 |.....e...3#...t| 
0000008b0  72 69 67 67 65 72 70 72  65 66 65 72 65 6e 63 65 |triggerpreference| 
0000008c0  73 5f 64 65 6c 65 74 65  64 70 72 65 66 65 72 65 |s_deletedprefere| 
0000008d0  6e 63 65 73 43 52 45 41  54 45 20 54 52 49 47 47 |ncesCREATE TRIGG| 
0000008e0  45 52 20 70 72 65 66 65  72 65 6e 63 65 73 5f 64 |ER preferences_d| 
0000008f0  65 6c 65 74 65 64 20 41  46 54 45 52 20 44 45 4c |eleted AFTER DEL| 
000000900  45 54 45 20 4f 4e 20 70  72 65 66 65 72 65 6e 63 |ETE ON preferenc| 
000000910  65 73 20 42 45 47 49 4e  20 44 45 4c 45 54 45 20 |es BEGIN DELETE | 
000000920  46 52 4f 4d 20 64 61 74  61 20 57 48 45 52 45 20 |FROM data WHERE |
```

.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;  
};
```

```
trainees-Mac:MacOS trainee$ hexdump -C 0xED  
00000000 ca fe ba be 00 00 02 01 00 00 07 80 00 00 03  
00000010 00 00 10 00 00 06 fd a0 00 00 00 0c 00 00 00 07  
00000020 00 00 00 03 00 07 10 00 00 06 72 a0 00 00 00 0c  
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
*  
00001000 cf fa ed fe 07 00 00 01 03 00 00 80 02 00 00 00  
00001010 17 00 00 00 70 10 00 00 85 00 01 00 00 00 00 00  
00001020 19 00 00 00 48 00 00 00 5f 5f 50 41 47 45 5a 45  
00001030 52 4f 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00001040 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  
00001050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00001060 00 00 00 00 00 00 00 00 19 00 00 00 b8 03 00 00  
00001070 5f 5f 54 45 58 54 00 00 00 00 00 00 00 00 00 00  
00001080 00 00 00 01 00 00 00 00 00 20 05 00 00 00 00 00  
00001090 00 00 00 00 00 00 00 00 00 20 05 00 00 00 00 00  
000010a0 07 00 00 00 05 00 00 00 0b 00 00 00 00 00 00 00  
000010b0 5f 5f 74 65 78 74 00 00 00 00 00 00 00 00 00 00  
000010c0 5f 5f 54 45 58 54 00 00 00 00 00 00 00 00 00 00  
000010d0 b0 10 00 00 01 00 00 00 20 38 03 00 00 00 00 00  
000010e0 b0 10 00 00 04 00 00 00 00 00 00 00 00 00 00 00  
000010f0 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00001100 5f 5f 73 74 75 62 73 00 00 00 00 00 00 00 00 00  
00001110 5f 5f 54 45 58 54 00 00 00 00 00 00 00 00 00 00  
00001120 d0 48 03 00 01 00 00 00 b8 02 00 00 00 00 00 00  
00001130 d0 48 03 00 01 00 00 00 00 00 00 00 00 00 00 00  
00001140 08 04 00 00 00 00 00 00 06 00 00 00 00 00 00 00  
00001150 5f 5f 73 74 75 62 5f 68 65 6c 70 65 72 00 00 00  
* _stub_helper...
```

Mach-O File Header

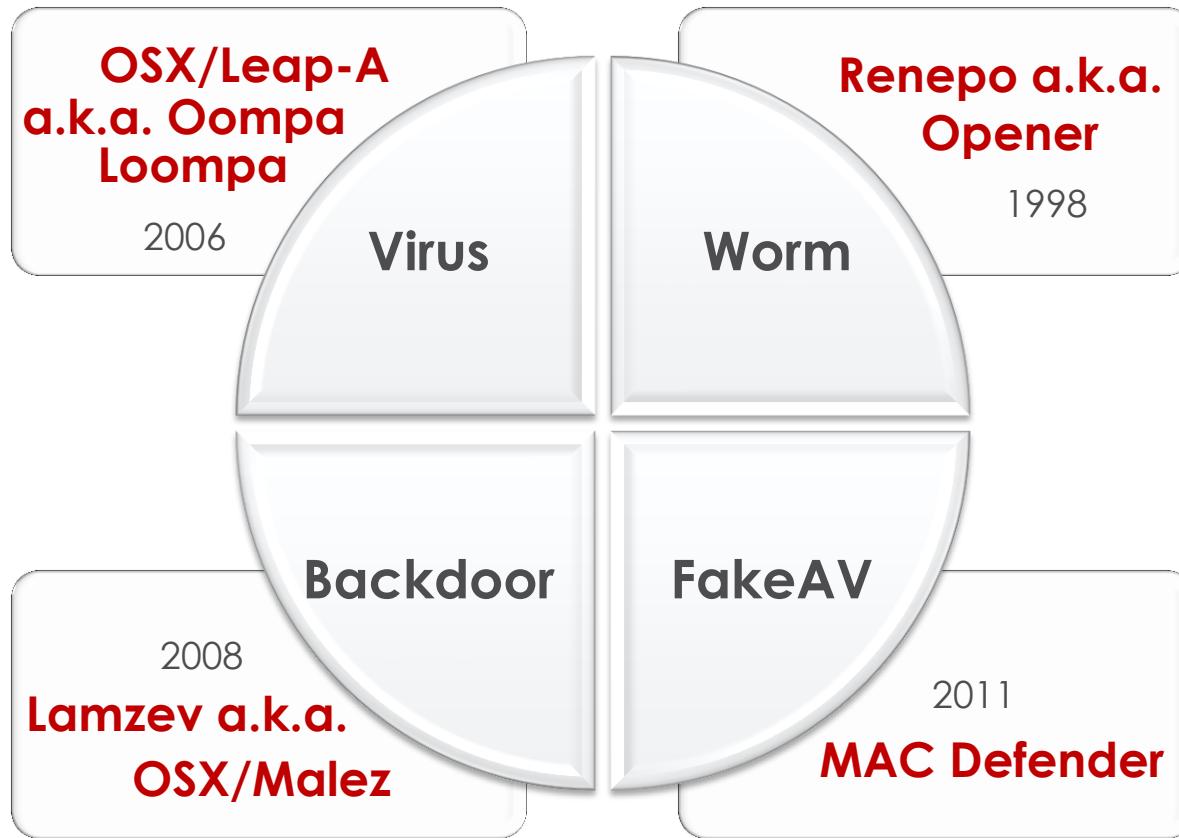
```
struct mach_header {  
    uint32_t magic;  
    cpu_type_t cputype;  
    cpu_subtype_t cpusubtype;  
    uint32_t filetype;  
    uint32_t ncmds;  
    uint32_t sizeofcmds;  
    uint32_t flags;  
    uint32_t reserved; /*available for 64-bit*/  
};
```

/* 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

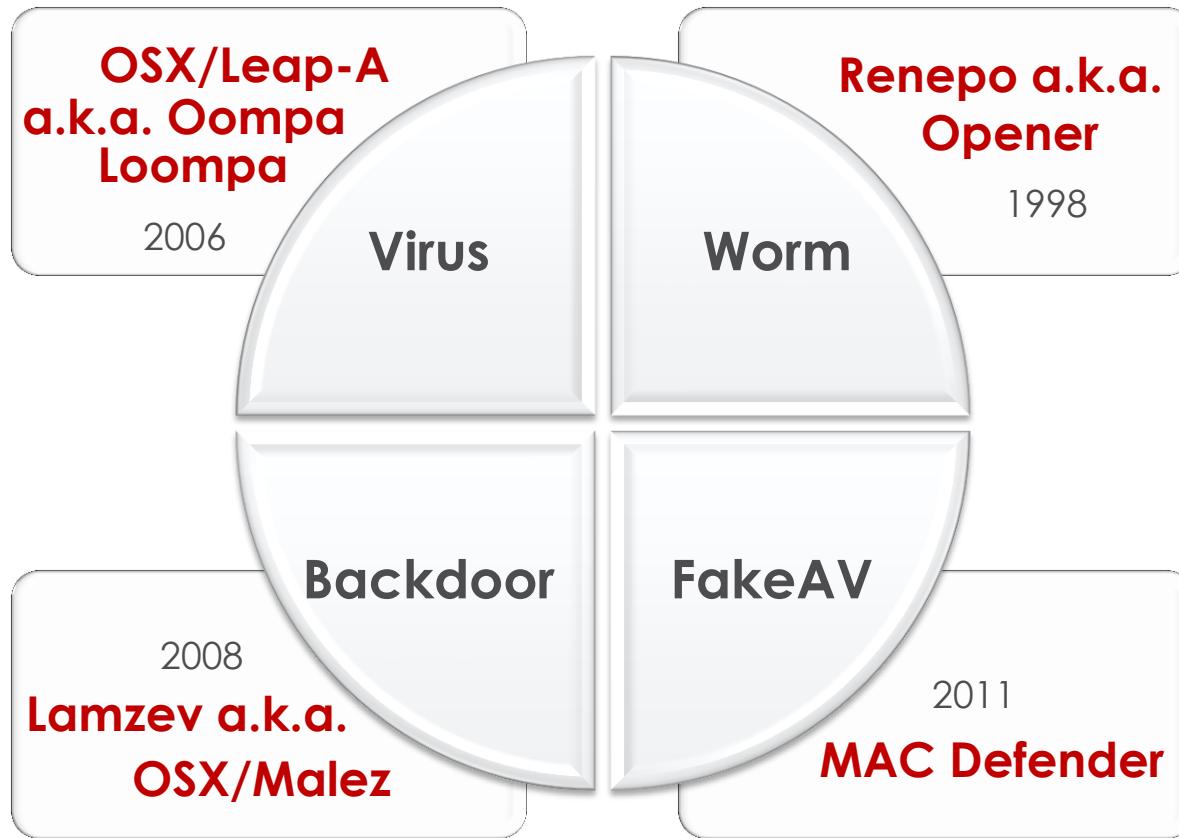


OSX/Leap-A a.k.a. Oompa Loompa

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

37 | Copyright 2015 Trend Micro Inc.

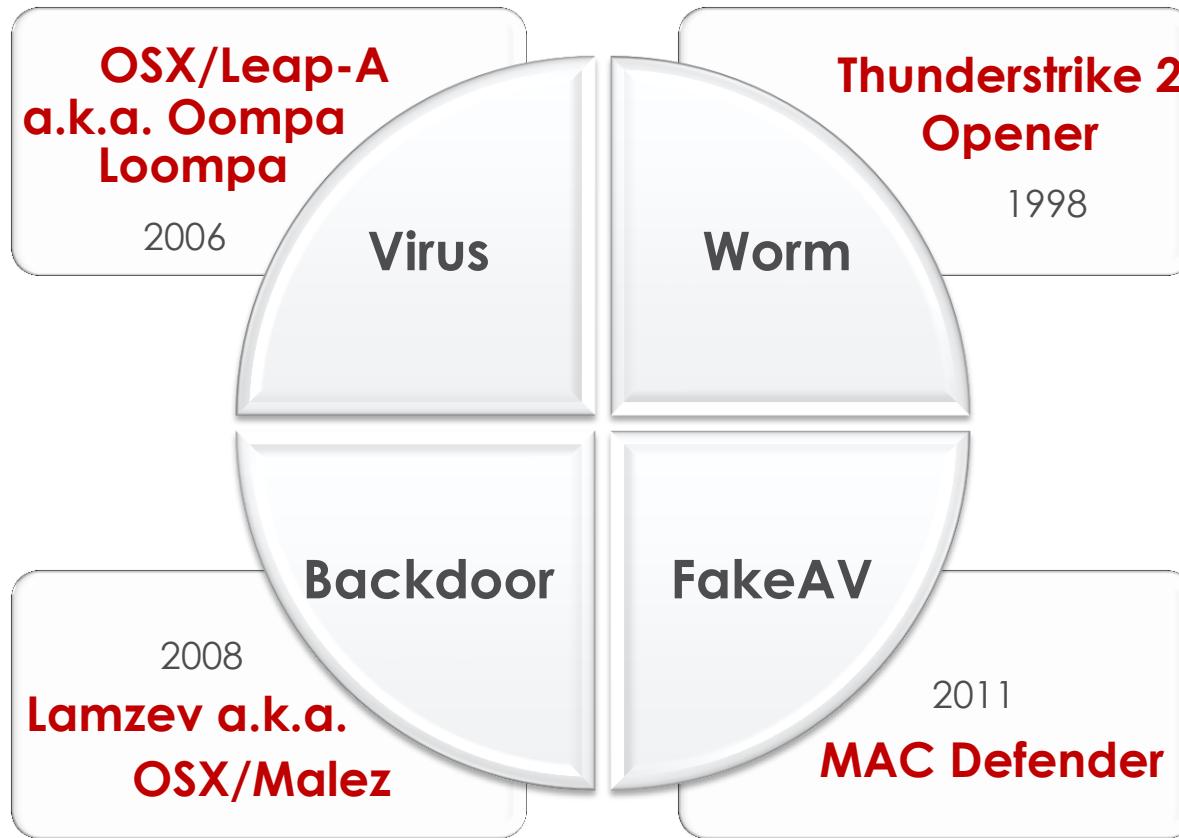
First MAC Malwares



Renepo a.k.a. Opener

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

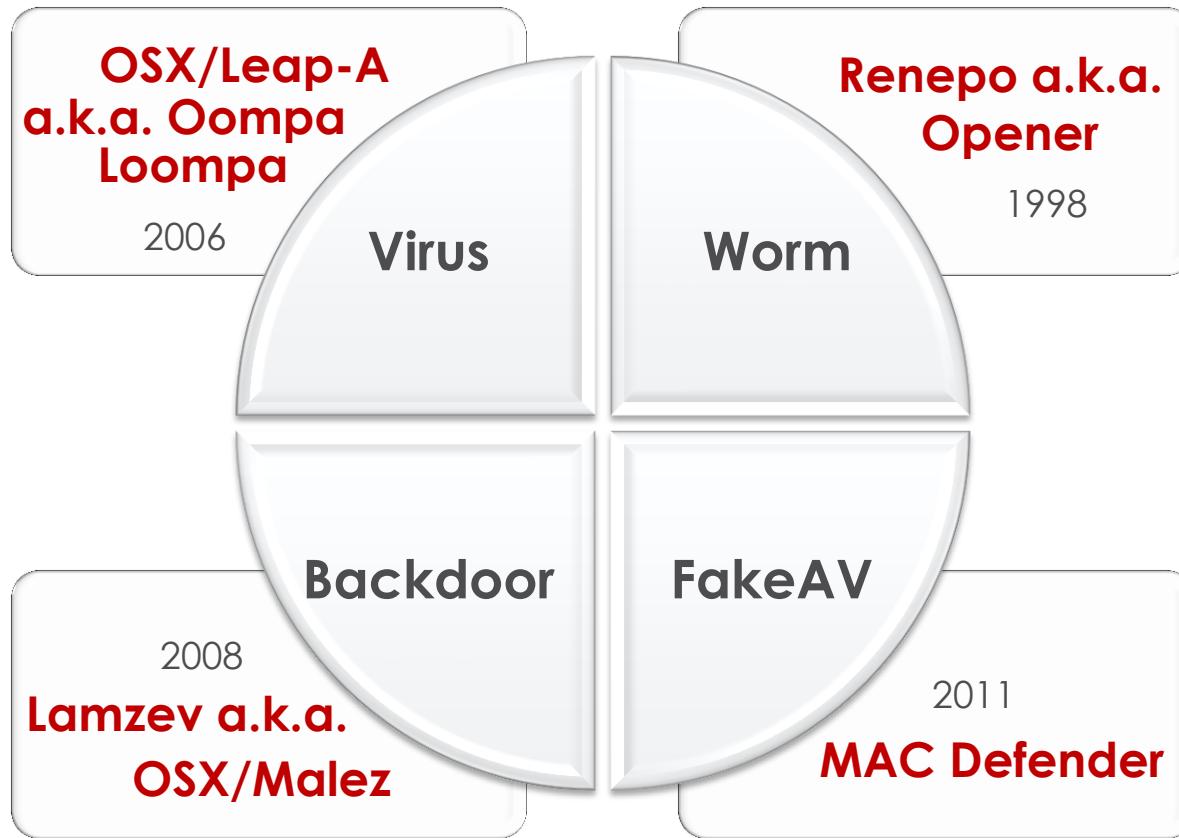
First MAC Malwares



Lamzev a.k.a.
OSX/Malez

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

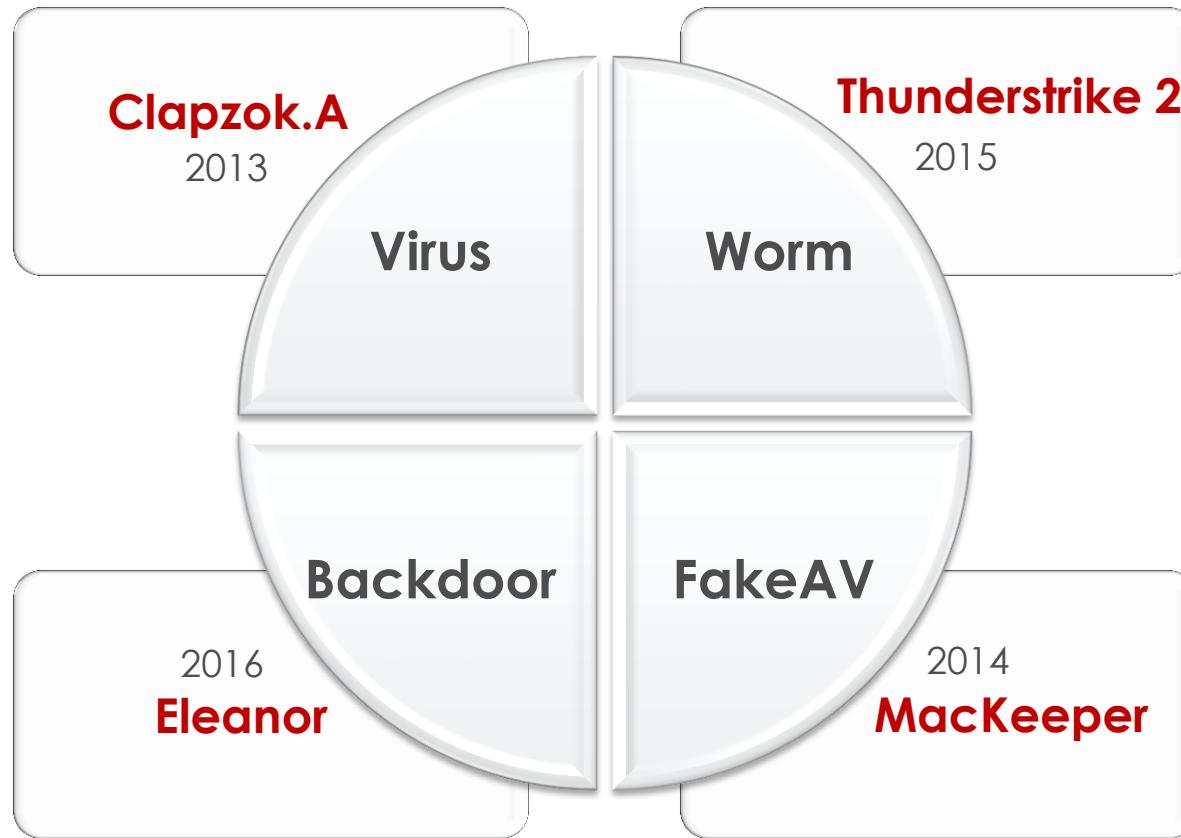
First MAC Malwares



MAC Defender

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

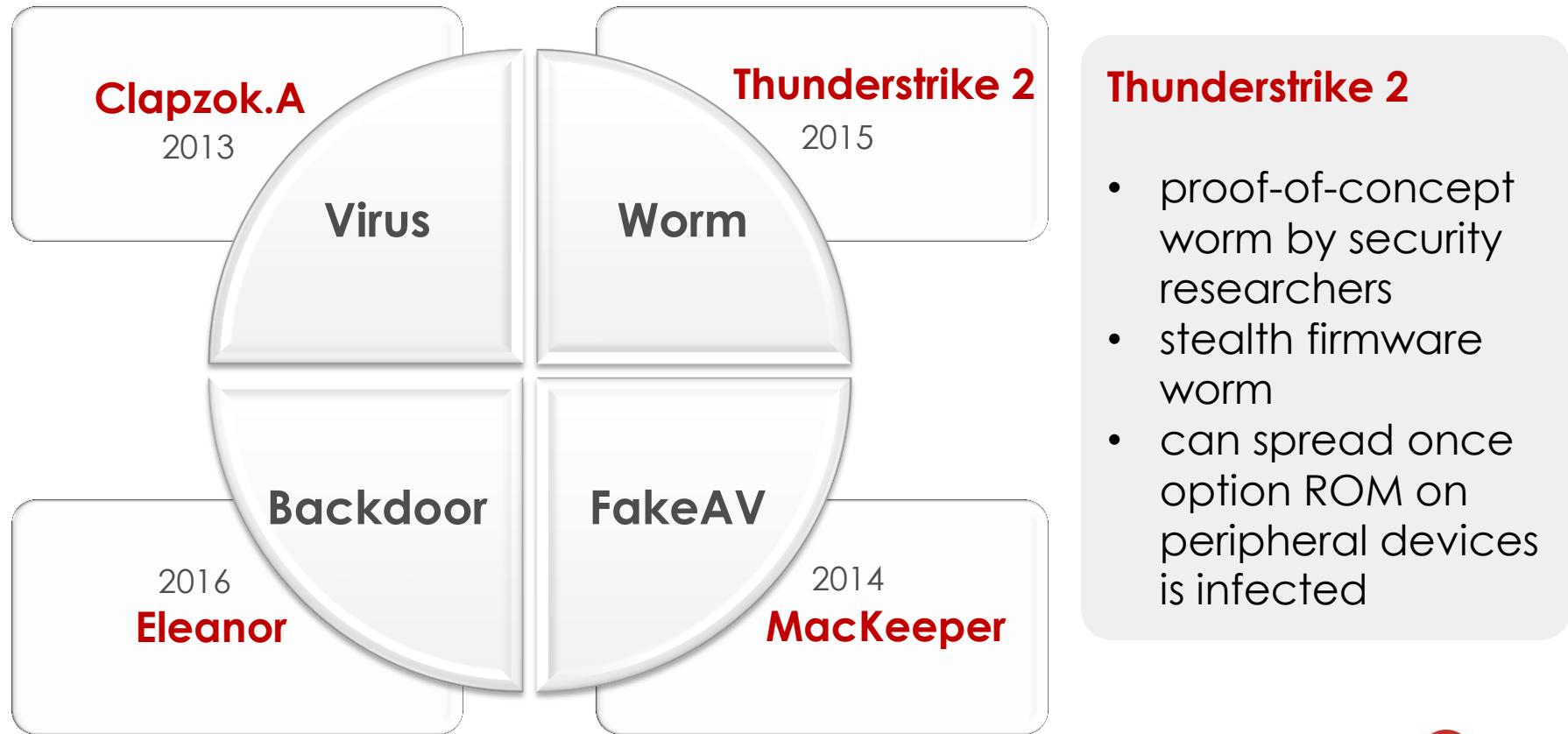
More Recent MAC Malwares



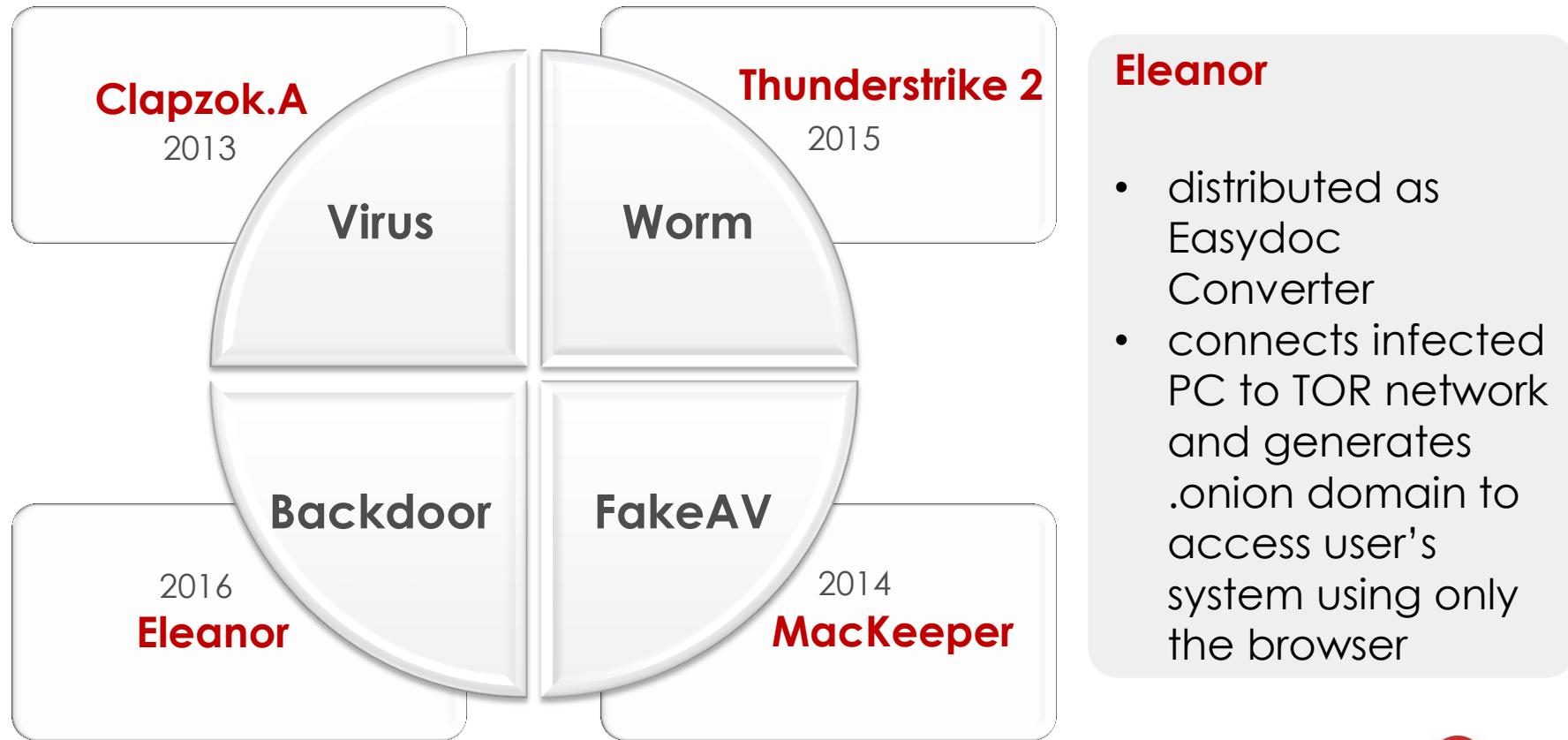
Clapzok.A

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

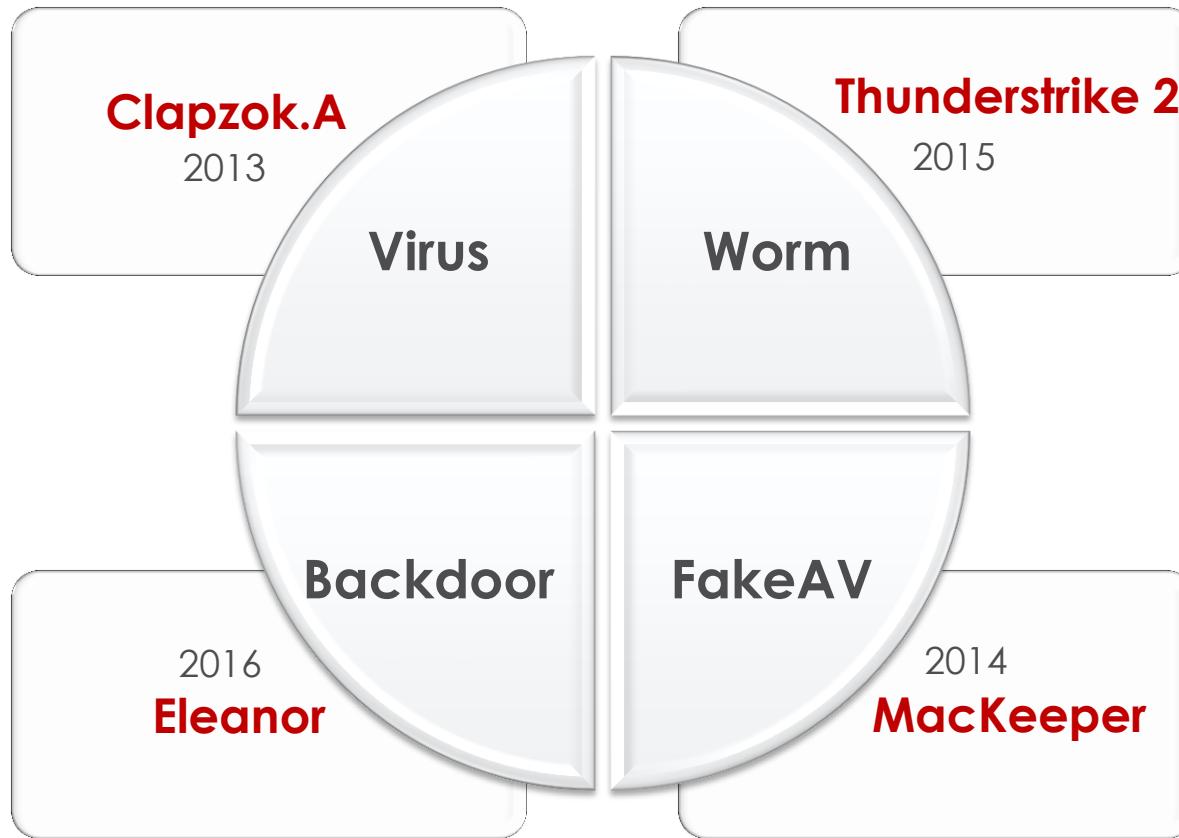
More Recent MAC Malwares



More Recent MAC Malwares



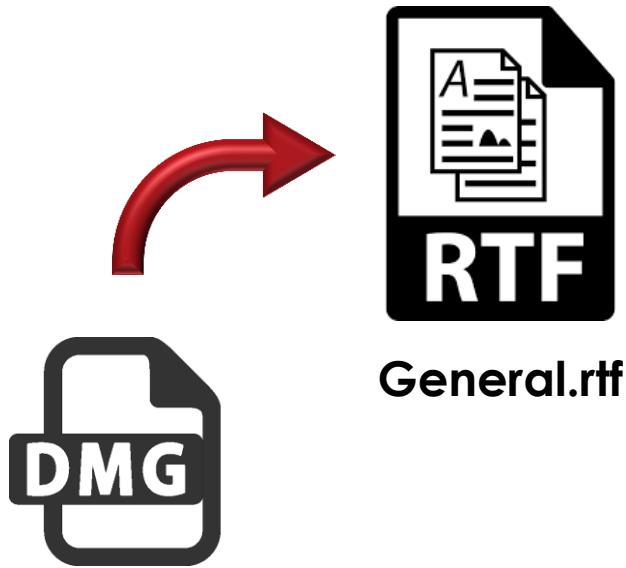
More Recent MAC Malwares



MacKeeper

- utility software for “MAC OS X security and optimization”

MAC Ransomware: KeRanger



Transmission v2.90
dmg installer

UPX-packed
Mach-O
Executable

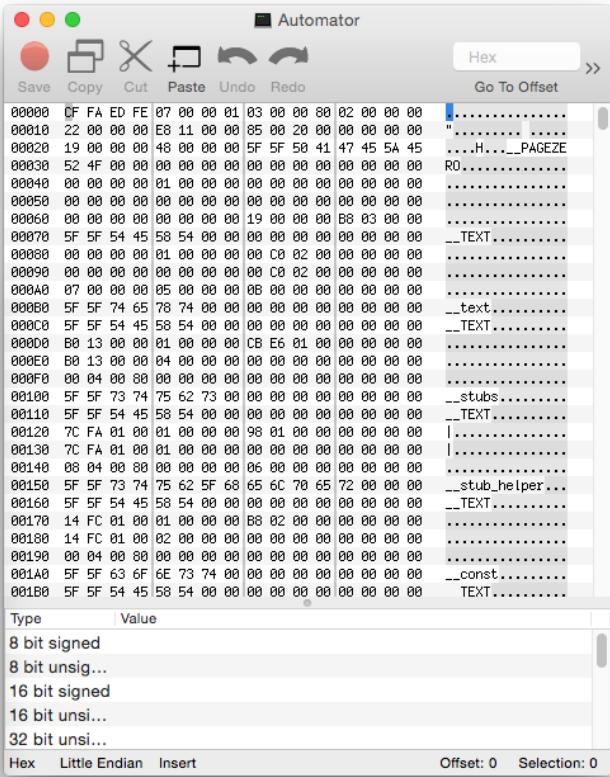
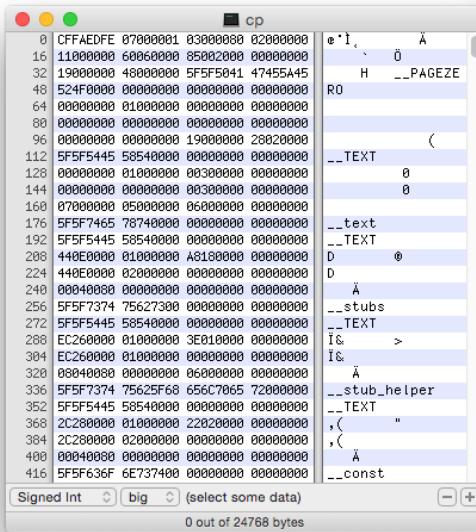
`kernel_pid;`
`kernel_time;`
`kernel_complete`

**encrypts users' files
and hold these for
ransom**

Tools For Static Analysis

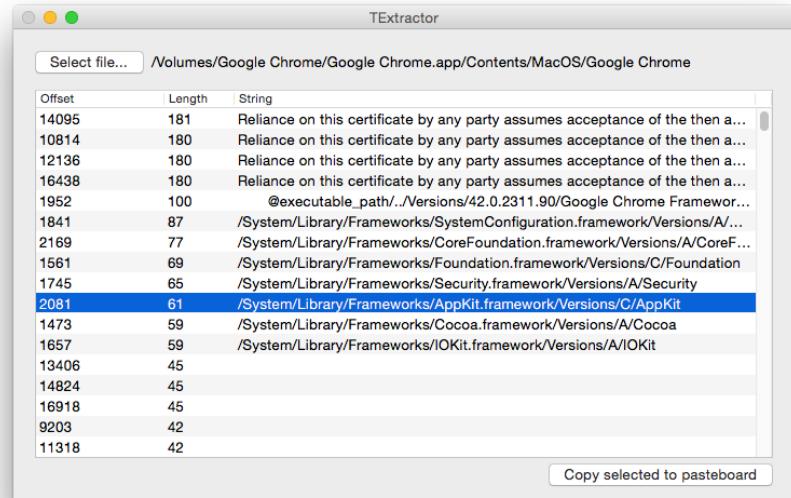
HexDumpers

- 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)

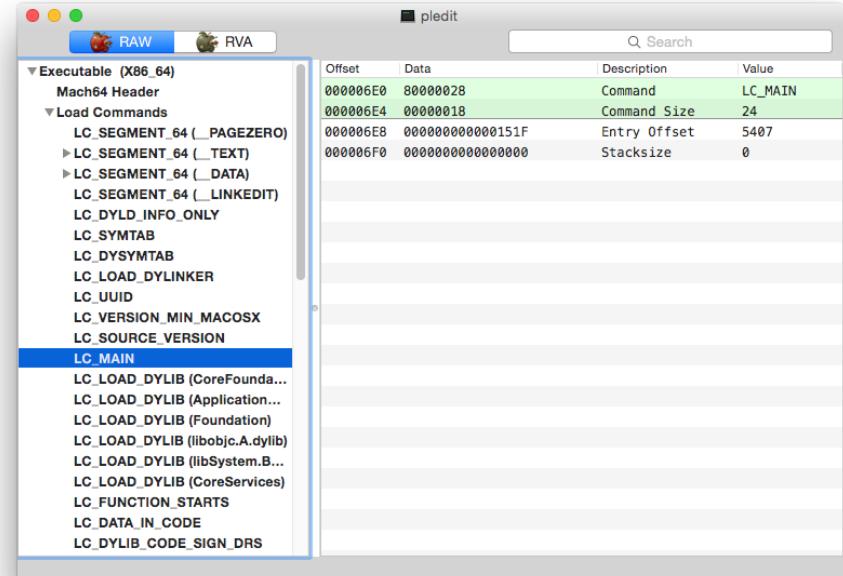


The screenshot shows the TExtractor application window. At the top, there is a "Select file..." button and the path "/Volumes/Google Chrome/Google Chrome.app/Contents/MacOS/Google Chrome". Below this is a table with three columns: Offset, Length, and String. The table lists several strings found in the file, with the row containing "/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit" highlighted in blue. A "Copy selected to pasteboard" button is located at the bottom right of the table area.

Offset	Length	String
14095	181	Reliance on this certificate by any party assumes acceptance of the then a...
10814	180	Reliance on this certificate by any party assumes acceptance of the then a...
12136	180	Reliance on this certificate by any party assumes acceptance of the then a...
16438	180	Reliance on this certificate by any party assumes acceptance of the then a...
1952	100	@executable_path../Versions/42.0.2311.90/Google Chrome Framework...
1841	87	/System/Library/Frameworks/SystemConfiguration.framework/Versions/A/...
2169	77	/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreF...
1561	69	/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation...
1745	65	/System/Library/Frameworks/Security.framework/Versions/A/Security
2081	61	/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit
1473	59	/System/Library/Frameworks/Cocoa.framework/Versions/A/Cocoa
1657	59	/System/Library/Frameworks/IOKit.framework/Versions/A/IOKit
13406	45	
14824	45	
16918	45	
9203	42	
11318	42	

Mach-O File Analysis Tools

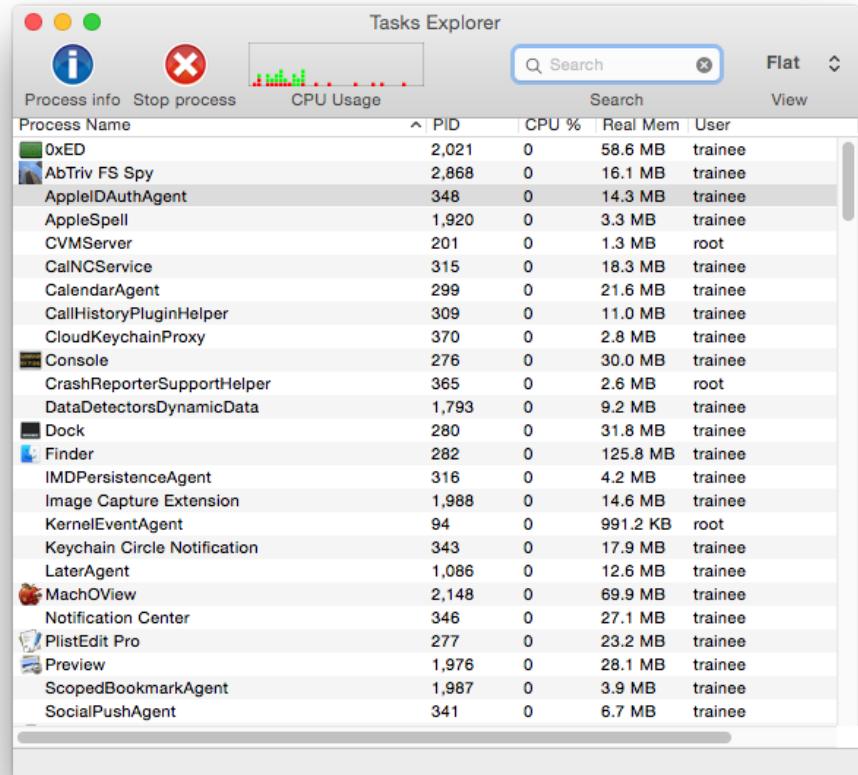
- Displays and parse the whole Mach-O file
 - MachOView.app (GUI)
 - Otool
 - machoviz.anrc-services.com



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'

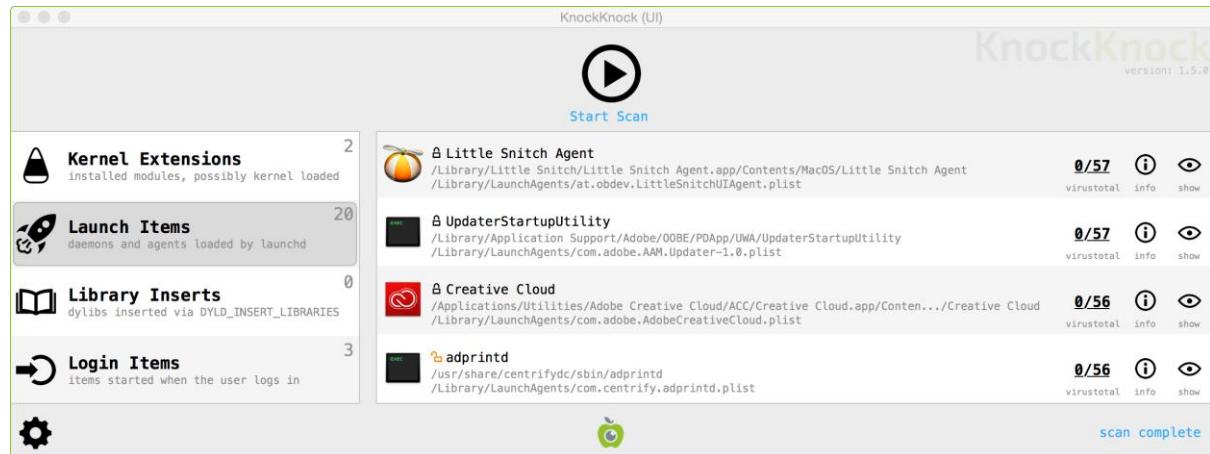


The screenshot shows the 'Tasks Explorer' application window on a Mac OS X desktop. The window has a title bar 'Tasks Explorer' with standard OS X window controls. Below the title bar is a toolbar with icons for 'Process info' (blue i), 'Stop process' (red X), and 'CPU Usage' (green/red bar chart). To the right of the toolbar are search fields ('Search' and 'Flat View' dropdown) and a 'View' button.

Process Name	PID	CPU %	Real Mem	User
0xED	2,021	0	58.6 MB	trainee
AbTriv FS Spy	2,868	0	16.1 MB	trainee
AppleIDAuthAgent	348	0	14.3 MB	trainee
AppleSpell	1,920	0	3.3 MB	trainee
CVMServer	201	0	1.3 MB	root
CalNCService	315	0	18.3 MB	trainee
CalendarAgent	299	0	21.6 MB	trainee
CallHistoryPluginHelper	309	0	11.0 MB	trainee
CloudKeychainProxy	370	0	2.8 MB	trainee
Console	276	0	30.0 MB	trainee
CrashReporterSupportHelper	365	0	2.6 MB	root
DataDetectorsDynamicData	1,793	0	9.2 MB	trainee
Dock	280	0	31.8 MB	trainee
Finder	282	0	125.8 MB	trainee
IMDPersistenceAgent	316	0	4.2 MB	trainee
Image Capture Extension	1,988	0	14.6 MB	trainee
KernelEventAgent	94	0	991.2 KB	root
Keychain Circle Notification	343	0	17.9 MB	trainee
LaterAgent	1,086	0	12.6 MB	trainee
MachOView	2,148	0	69.9 MB	trainee
Notification Center	346	0	27.1 MB	trainee
PlistEdit Pro	277	0	23.2 MB	trainee
Preview	1,976	0	28.1 MB	trainee
ScopedBookmarkAgent	1,987	0	3.9 MB	trainee
SocialPushAgent	341	0	6.7 MB	trainee

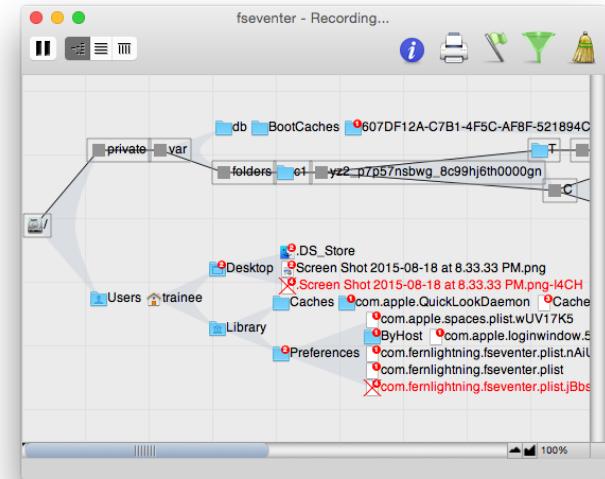
Persistence Monitoring

- Display launch daemons or agents
 - launchctl 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

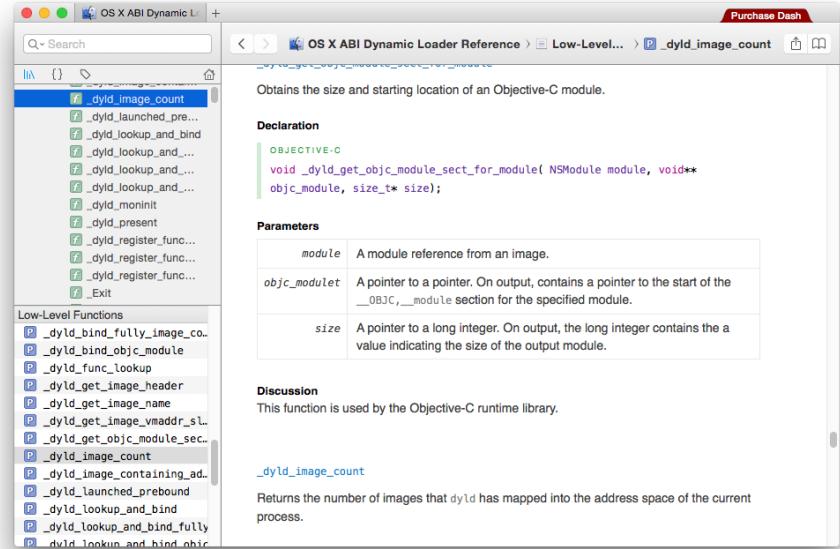


Network Monitoring

- 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/leapFAQ.html>
- <http://reverse.put.as/2013/05/31/clapzok-a-reversing-the-os-x-part-of-a-multiplatform-poc-infecto/>

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

Thank you!!!
