Shifting Paradigms from Windows to Mac

Nicholas Ramos and Michelle Morales
Introduction to MAC OS X
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
*Market share data is only between Mac and Windows, other operating systems are excluded
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

Boot ROM firmware activated

Power-On Self Test (POST)
MAC Boot-Up

EFI selects OS to use

control is passed on to boot.efi loader

Boot loader loads kernel environment

kernel cache → mkext cache → /System/Library/Extensions
MAC Boot-Up

boot loader starts kernel's initialization

initialize MAC and BSD data structures → initialize I/O kit

kernel looks for root device and roots BSD off of it
MAC Boot-Up

launchd process spawns important WindowServer processes

launchd starts loginwindow.app
MAC Boot-Up
Auto-Start Mechanism

TRICKS AND WAYS FOR MALWARE PERSISTENCE
Pre-Login Persistence

EFI

XNU (kernel)

Kernel Cache
Launched as Daemon or Agent

launchd

Daemon

/System/Library/LaunchDaemons
/Library/LaunchDaemons

Agent

/System/Library/LaunchAgents
/Library/LaunchAgents

~/Library/LaunchAgents
## Type of Launched Daemons and Agents

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

```c
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

```c
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
- 2006

Renepo a.k.a. Opener
- 1998

Lamzev a.k.a. OSX/Malez
- 2008

MAC Defender
- 2011

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

OSX/Leap-A a.k.a. Oompa Loompa
2006

Renepo a.k.a. Opener
1998

Lamzev a.k.a. OSX/Malez
2008

MAC Defender
2011
First MAC Malwares

- OSX/Leap-A a.k.a. Oompa Loompa
  - 2006
- Thunderstrike 2 Opener
  - 1998
- Lamzev a.k.a. OSX/Malez
  - 2008
- MAC Defender
  - 2011

Lamzev a.k.a. OSX/Malez

- hacker tool to install backdoor
- needs physical access to the system
First MAC Malwares

- **OSX/Leap-A a.k.a. Oompa Loompa**
  - 2006

- **Renepo a.k.a. Opener**
  - 1998

- **Lamzev a.k.a. OSX/Malez**
  - 2008

- **MAC Defender**
  - 2011

**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**
  - 2013
- **Thunderstrike 2**
  - 2015
- **Eleanor**
  - 2016
- **MacKeeper**
  - 2014

**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

- Clapzok.A (2013)
- Thunderstrike 2 (2015)
- Eleanor (2016)
- MacKeeper (2014)

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

- **Clapzok.A**
  - 2013

- **Thunderstrike 2**
  - 2015

- **Backdoor**
  - 2016
  - **Eleanor**

- **FakeAV**
  - 2014
  - **MacKeeper**

**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

- **Clapzok.A**
  - 2013

- **Thunderstrike 2**
  - 2015

- **Eleanor**
  - 2016

- **MacKeeper**
  - 2014
  - 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;
kernl_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 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
- 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://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

BACKDOOR

FAKEAV
- https://discussions.apple.com/docs/DOC-3036

RANSOMWARE

macOS Sierra
Thank you!!!