Mac-A-Mal
An Automated Framework for Mac Malware Hunting

Pham Duy Phuc†
Fabio Massacci ‡

Sfylabs†
University of Trento‡
Motivation

- Mac OS market share is increasing 🍃
- Increasing number of new Mac malware
- Increasing complexity of Mac threats
- Common techniques to analyze malware using sandbox technologies on Windows, Linux, Android, macOS.
  → Develop a auto malware analysis framework on macOS.
Malware analysis for macOS

- Static analysis
- Dynamic analysis
- Meet Cuckoo!
Mac-A-Mal static analysis

- Binary information: Header; CODE, DATA segments; DYLIB; LOAD commands; Symbol table.
- Entropy
- Signature information
- BoM information for DMG/APP archive
- Plist information
Mac-A-Mal dynamic analysis

Monitor machine (MacOS)
- Kernel space
  - Log syscall
  - Log process exec
  - Log file operations
  - KEXT sockets
- Userspace
  - Malware
  - Daemon sockets
  - Analysis agent

Analysis machine
- Cuckoo Frontend
  - Web panel
  - Storage & reports
  - Elastic search
  - YARA/VT query
- Analyzer
  - Distribute sample
  - Behavioral analysis
  - Behavioral signature
- Network driver
  - TCPDump

Internet | Host-only | Net Emulation
Any file types are supported

- `/usr/bin/open - mac_syscall interface`
- `hdiutil – mount Apple disk image`
- `Java – Perl – Python`
- Archive
- URL
Kernel-space monitor

- Resolve macOS kernel protection: Onyx the black cat & Grey-fox
- Syscall interception and arguments collection
- Process tracing, XPC Services tracing
- File accessed behaviors
- Network syscall
Detect evasion techniques & mitigation

- Detect Anti-debug:
  - By intercept → ptrace(), sysctl()
- Mitigate Anti-sandbox:
  - SIP status manipulation → csrctl()
  - Hardening process names, virtual devices information (display resolution, processor cores, etc.) → sysctl(), ioctl()
  - Harden VM configuration (e.g: CPUID, VM Plist)
(no) Human Interaction

Authorization Solver
• Quartz: CGEventCreateKeyboardEvent

Screenshots & Interact MessageBox:
• Quartz: CGWindowListCreateImage, CGEventCreateMouseEvent
OSX/Mughthesec

Static analysis
Developer code signer
Quoc Thinh 9G2J3967H9
Pham Huong 2BS26F3ZCP
Phan Anh C7J9SJ95GX
Nhien Nguyen
Thanh Thuy WAA98JBA59
Tran Phong GMFY4TULB3
Minh Duc 7CxEE5FM69W
Mai Linh M3XXTCHY66

Dynamic analysis
Evasion by detecting network driver MAC address
Persistence indicator: mughthesec.plist

Network
Suspicious domains
appfastplay.com
mughthesec.com
SimplyEApps.com
dynacubeapps.com
cloudmacfront.com
api.airautoupdates.com
osxessentials.com
api.vertizoom.com
macgabspan.com
install.searchwebsvc.com
trustedsafefinder.com

What makes the campaign interesting?

#1
Fake Adobe Flash install
Free bonus:
- Advanced Mac cleaner
- Safe search Safari Extension
- Booking.com

#2
8 Vietnamese valid Apple developer ID (only 2 revoked) ~$800

#3
97% undetected on VirusTotal (over 71 found samples)

#4
Staying undetected at least 4 months,
>10 domains participated, Drive-by CDN hosting

Screenshot(s)
On large scale

- $N=2149$
- 85% of the collected samples are adware, which dominated by OSX/Pirrit and OSX/MacKeeper
- 86 different Mac malware families, and 49% of them belongs to backdoor/trojan.
macOS malware evolution
Summary

• It is possible to automatically analyze network traffic, malware evasion techniques, persistence methods, file operations etc. from samples in virtualized Mac environment.
• We succeeded in clarifying malware variants and its evolution on macOS
• Found undiscovered Mac adware including legitimate Apple developer certificates, other undetected backdoor (APT32) → possibility of outperforming existing solutions currently available on the market.
• Opensource: https://github.com/phdphuc/mac-a-mal
Q&A