

# Latinoware 2015

## MACH-O A NEW THREAT

Ricardo Amaral a.k.a L0gan



# \$Whoami

---

## Ricardo L0gan

Security Specialist with over 15 years of experience, enthusiastic in malware research, pen-test and reverse engineering. I've a solid knowledge on topics like network security, hardening and tuning across multiple platforms such as Windows, Linux, OS X and Cisco. Beginner in programming languages as Python, C and Assembly.

In Brazil I contribute to the Slackware community (Slackshow and Slackzine) and I'm member of the Staff of some events: H2HC, SlackShow and Bsides SP.



**### Long live Open Source - Use Linux (Slackware) ###**



# Agenda

---

**0x00** Motivation of Research

**0x01** OS X, The New Target

**0x02** The Mach-O Format

**0x03** Tools For Analysis (Static / Dynamic)

**0x04** Current Threats

**0x05** Conclusions



## 0x00 - Motivation of Research



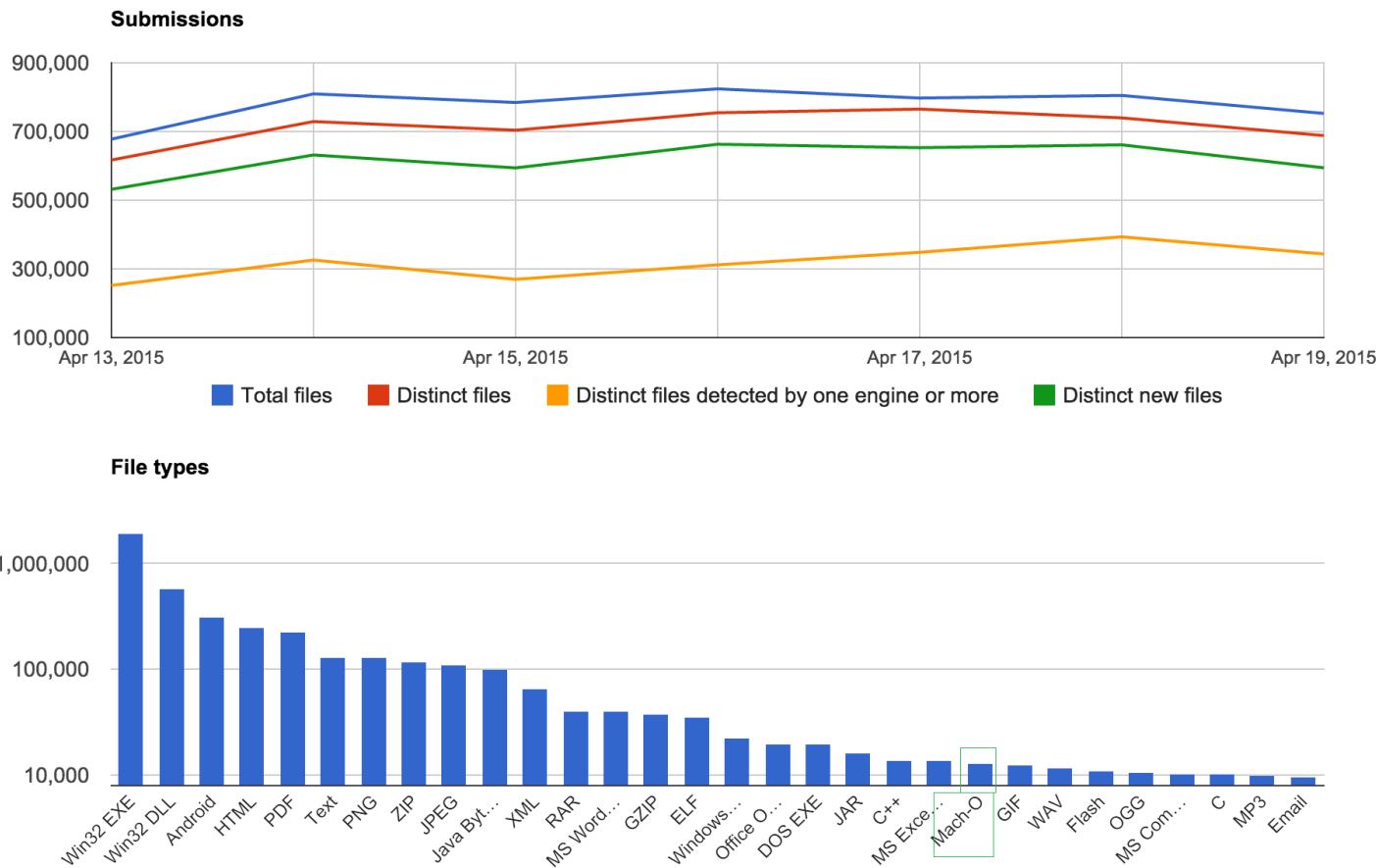
Windows always gets infected!!!

Does Linux ever gets infected??

“Mac OS ever gets infected...”



# 0x01 – OS X, The New Target



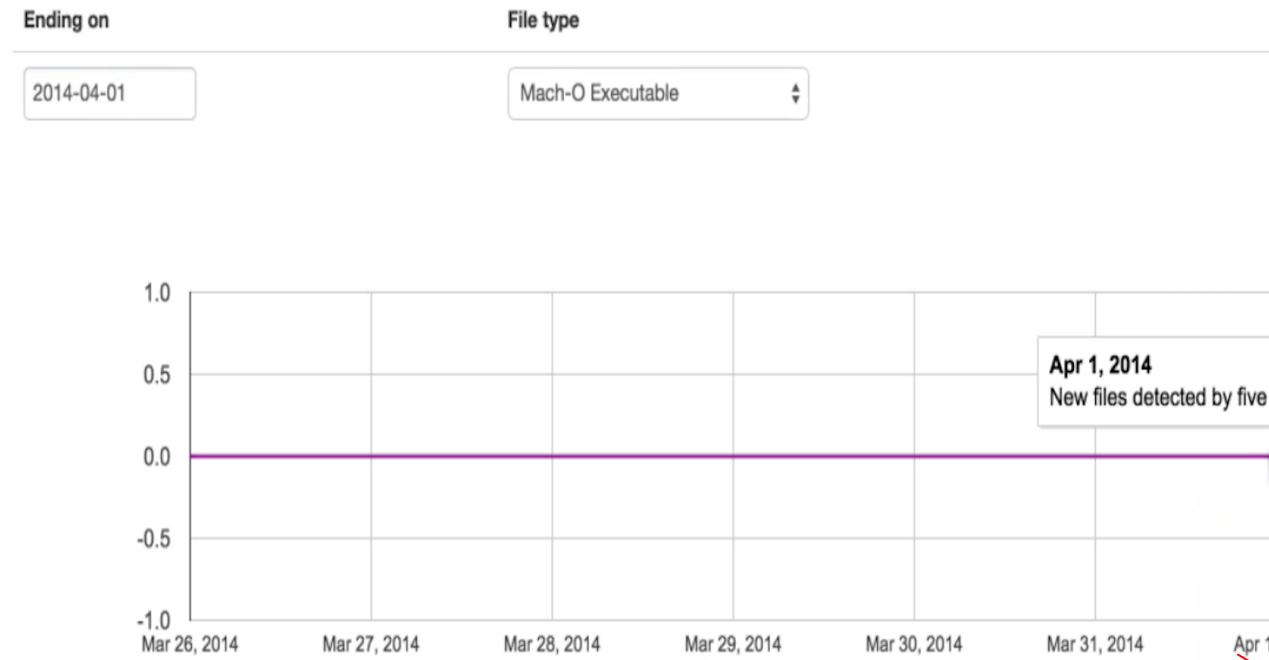
Source: [www.virustotal.com](http://www.virustotal.com)



# 0x01 – OS X, The New Target

## Processed files

The following graph displays some global trends regarding the total number of files processed by virustotal. You may focus on particular file types.



Source: [www.virustotal.com](http://www.virustotal.com)

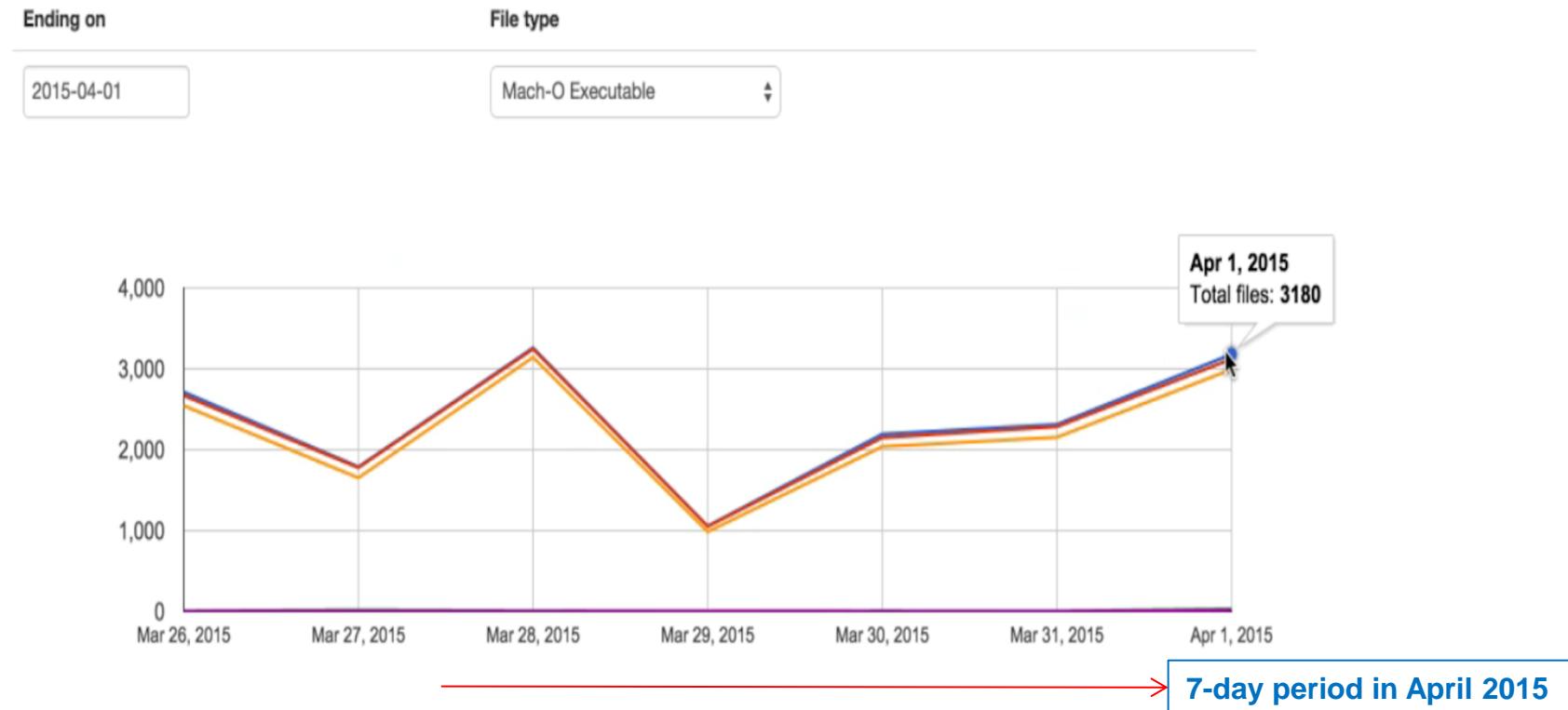
7-day period in April 2014



# 0x01 – OS X, The New Target

## Processed files

The following graph displays some global trends regarding the total number of files processed by virustotal. You may focus on particular file types.



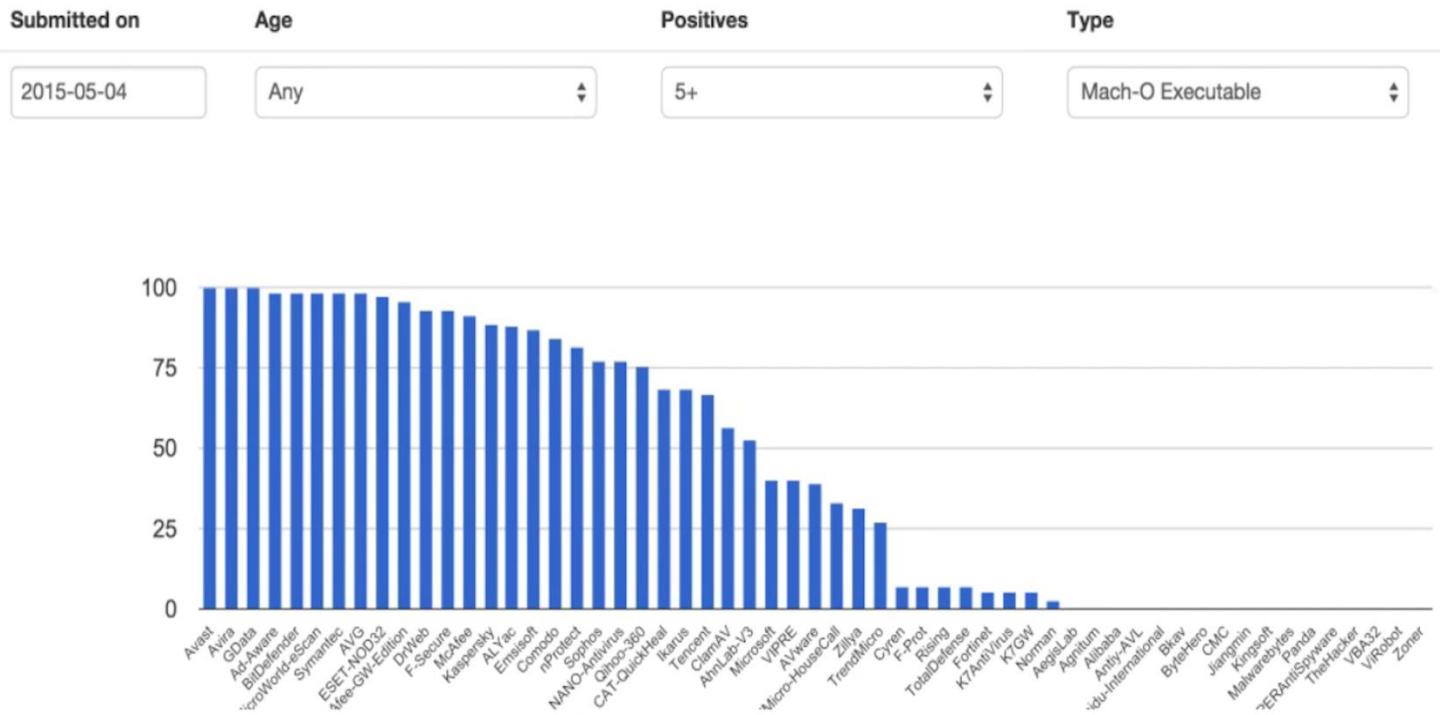
Source: [www.virustotal.com](http://www.virustotal.com)



# 0x01 – OS X, The New Target

## Detection ratios by vendor

The following chart displays the detection performance by vendor regarding files matching a given age, file type and total detection count criteria. In other words, of all files matching the given criteria that have been processed by the given engine, what percentage of them were detected by the engine under consideration?



Source: [www.virustotal.com](http://www.virustotal.com)

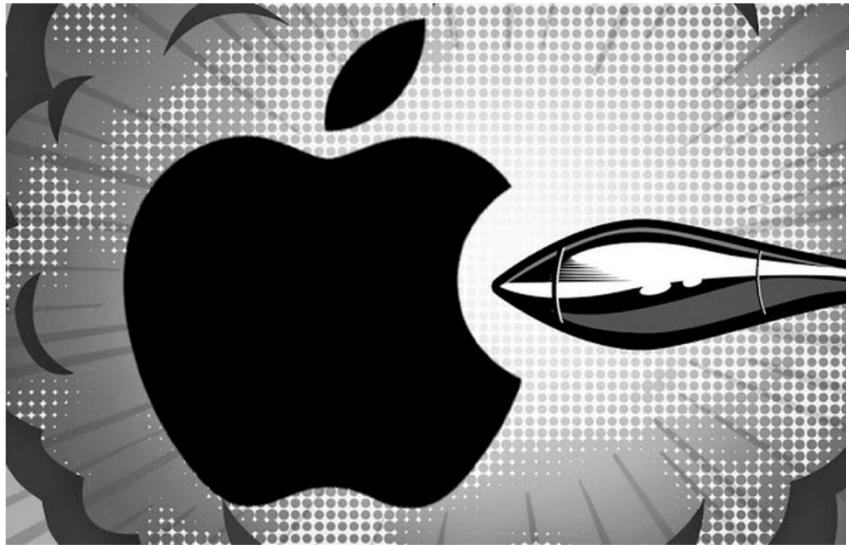


# 0x01 – OS X, The New Target

Windows? NO, Linux and Mac OS X Most Vulnerable

## Operating System In 2014

Tuesday, February 24, 2015 by Swati Khandelwal



Source: <http://thehackernews.com/2015/02/vulnerable-operating-system.html>



Revoltado com a Apple, hacker do mundo jailbreak publica detalhes de uma falha de segurança do OS X

Rafael Fischmann 23/07/2015 às 09:31



# 0x01 – OS X, The New Target

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

Source: <http://thehackernews.com/2015/02/vulnerable-operating-system.html>



## 0x02 - The Mach-O Format

### Binary (Linux)

```
logan@Slack-Hack-14 ~ $  
logan@Slack-Hack-14 ~ $ file /usr/bin/cal  
/usr/bin/cal: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), stripped  
logan@Slack-Hack-14 ~ $
```

### Binary (Windows)

```
loganbr ~/Downloads $  
loganbr ~/Downloads $ file calc.exe  
calc.exe: PE32+ executable for MS Windows (GUI) Mono/.Net assembly  
loganbr ~/Downloads $
```

### Binary (OS X)

```
loganbr ~/Downloads $ file /usr/bin/cal  
/usr/bin/cal: Mach-O 64-bit executable x86_64  
loganbr ~/Downloads $
```



## 0x02 - The Mach-O Format

---

The mach-o format was adopted as the **standard** in OS X from version 10.6 on

We are currently in version 10.11 (~~Yosemite~~-El Capitan).



## 0x02 - The Mach-O Format

CA FE BA BE - Mach-O Fat Binary

FE ED FA CE - Mach-O binary (32-bit)

FE ED FA CF - Mach-O binary (64-bit)

CE FA ED FE - Mach-O binary (reverse byte 32-bit)

CF FA ED FE - Mach-O binary (reverse byte 64-bit)



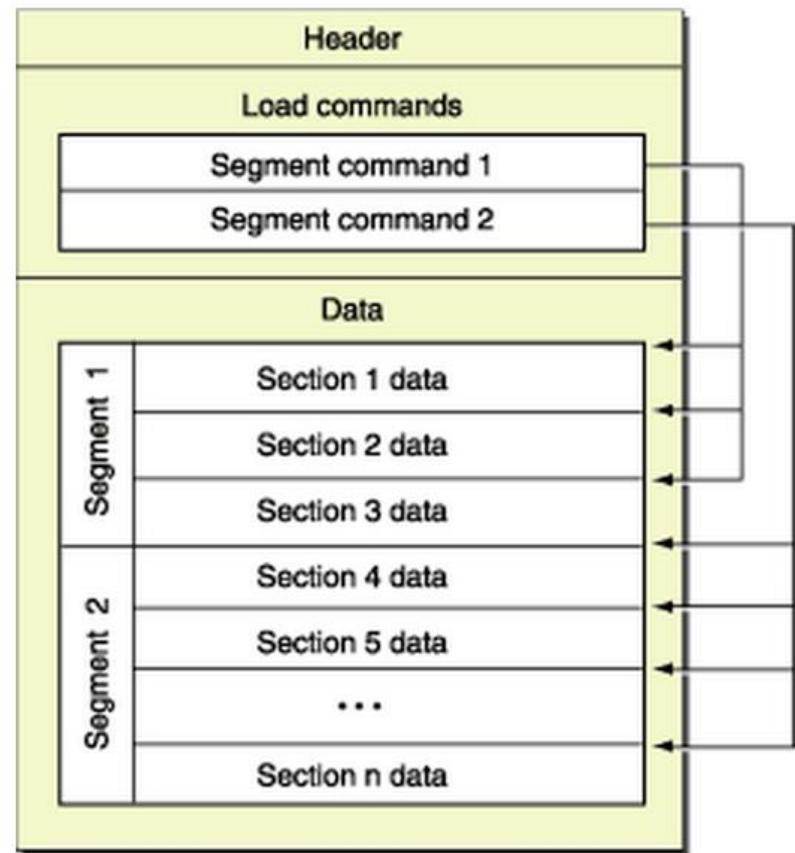
# 0x02 - The Mach-O Format

Mach-O (Mach Object)

HEADER  
LOAD COMMANDS  
SECTIONS

Architecture of object code

ppc ppc64 i386 x86\_64 armv6  
armv7 armv7s arm64





## 0x02 - The Mach-O Format

HEADER

```
loganbr ~ $ vim /usr/include/mach-o/loader.h
```

```
/*
 * The 64-bit mach header appears at the very beginning of object files for
 * 64-bit architectures.
 */
struct mach_header_64 {
    uint32_t    magic;        /* mach magic number identifier */
    cpu_type_t   cputype;     /* cpu specifier */
    cpu_subtype_t cpusubtype; /* machine specifier */
    uint32_t    filetype;    /* type of file */
    uint32_t    ncmds;        /* number of load commands */
    uint32_t    sizeofcmds;   /* the size of all the load commands */
    uint32_t    flags;        /* flags */
    uint32_t    reserved;    /* reserved */
};
```



## 0x02 - The Mach-O Format

LOAD COMMANDS

```
loganbr ~ $ vim /usr/include/mach-o/loader.h
```

```
struct load_command {  
    uint32_t cmd;          /* type of load command */  
    uint32_t cmdsize;      /* total size of command in bytes */  
};
```



## 0x02 - The Mach-O Format

SECTIONS

```
loganbr ~ $ vim /usr/include/mach-o/loader.h
```

```
struct section_64 { /* for 64-bit architectures */
    char          sectname[16];   /* name of this section */
    char          segname[16];   /* segment this section goes in */
    uint64_t      addr;        /* memory address of this section */
    uint64_t      size;        /* size in bytes of this section */
    uint32_t      offset;      /* file offset of this section */
    uint32_t      align;       /* section alignment (power of 2) */
    uint32_t      reloff;      /* file offset of relocation entries */
    uint32_t      nreloc;      /* number of relocation entries */
    uint32_t      flags;       /* flags (section type and attributes)*/
    uint32_t      reserved1;   /* reserved (for offset or index) */
    uint32_t      reserved2;   /* reserved (for count or sizeof) */
    uint32_t      reserved3;   /* reserved */
};
```



# 0x03 – Tools For Analysis (Static / Dynamic)

## Static Analysis

- file
- strings
- hex editor (**graphical**)
- lipo
- otool
- nm
- codesign
- machOView (**graphical**)
- hopper (**graphical**)
- class-dump

## Dynamic Analysis

- xcode (**graphical**)
- IDA Pro (**graphical**)
- llDb
- fseventer
- open snoop
- activity Monitor (**graphical**)
- procoxp
- tcpdump
- cocoaPacketAnalyzer (**graphical**)
- wireshark (**graphical**)
- lsocK
- little Snitch



# 0x03 – Tools For Analysis (Static)

FILE

```
logan /opt/malware/mach-o $ file *
malware:      directory
malware.zip: Zip archive data, at least v1.0 to extract
old:          directory
sample_01:    Mach-O universal binary with 3 architectures
sample_01 (for architecture x86_64):    Mach-O 64-bit executable x86_64
sample_01 (for architecture i386):       Mach-O executable i386
sample_01 (for architecture ppc7400):   Mach-O executable ppc
sample_02:    Mach-O executable i386
sample_03:    Mach-O executable i386
sample_04:    Mach-O executable i386
sample_05:    Mach-O universal binary with 2 architectures
sample_05 (for architecture armv7):     Mach-O executable arm
sample_05 (for architecture armv7s):    Mach-O executable arm
sample_06:    Mach-O 64-bit executable x86_64
sample_07:    Mach-O universal binary with 2 architectures
sample_07 (for architecture armv7):     Mach-O executable arm
sample_07 (for architecture armv7s):    Mach-O executable arm
sample_08:    Mach-O executable i386
sample_09:    Mach-O executable ppc
sample_10:    Mach-O universal binary with 2 architectures
sample_10 (for architecture i386):      Mach-O executable i386
sample_10 (for architecture ppc7400):   Mach-O executable ppc
logan /opt/malware/mach-o $
```

mach-o



## 0x03 – Tools For Analysis (Static)

STRINGS

```
logan /opt/malware/mach-o $ strings sample
IODeviceTree
text/html; charset=utf-8
;/?:@8=-+$
%e-%e&
POST
application/x-www-form-urlencoded; charset=utf-8
Content-Type
text/html
Accept
no-cache
Cache-Control
Pragma
close
Connection
something is wrong: %e
CFBundleExecutable
http://www.comeinbaby.com/start_log/?app=%e&sn=%e
serial-number
kill -HUP SpringBoard
mv "%e" "%e"
_OBJC_AutoreleasePoolPush
_OBJC_AutoreleasePoolPop
__TEXT
__LINKEDIT
_OBJC_SetInstanceVariable
_OBJC_SetIvar
_OBJC_Copy
_OBJC_Retain
_OBJC_RetainBlock
_OBJC_Release
```



# 0x03 – Tools For Analysis (Static)

The screenshot shows four windows side-by-side:

- HexEdit**: Top-left window showing a hex dump of memory starting at address 00000000. The bytes CA FE BA BE are highlighted in yellow.
- wxHexEditor**: Top-right window showing a hex dump of memory starting at address 00000000. The bytes CA FE BA BE are highlighted in yellow.
- OxED**: Middle-right window showing a hex dump of memory starting at address 00000000. The bytes CA FE BA BE are highlighted in yellow.
- InfoPath**: Bottom-right window showing a table of file metadata. It includes columns for Path, Type, and Value. Key entries include:
  - Type: 8 bit signed, Value: -54
  - Type: 8 bit unsig..., Value: 0xCA
  - Type: 16 bit signed, Value: -310
  - Type: 16 bit unsi..., Value: 0xFECA
  - Type: 32 bit unsi..., Value: 0XBEBAFECA
  - Type: 32 bit signed, Value: -1095041334
  - Type: 64 bit unsi...

HEX EDITOR

HexEdit

wxHexEditor

0xED



## 0x03 – Tools For Analysis (Static)

```
logan /opt/malware/mach-o $ lipo -detailed_info sample
Fat header in: sample
fat_magic 0xcafebabe
nfat_arch 2
architecture armv7
    cputype CPU_TYPE_ARM
    cpusubtype CPU_SUBTYPE_ARM_V7
    offset 16384
    size 57824
    align 2^14 (16384)
architecture armv7s
    cputype CPU_TYPE_ARM
    cpusubtype CPU_SUBTYPE_ARM_V7S
    offset 81920
    size 57824
    align 2^14 (16384)
logan /opt/malware/mach-o $ lipo -detailed_info sample_10
Fat header in: sample_10
fat_magic 0xcafebabe
nfat_arch 2
architecture i386
    cputype CPU_TYPE_I386
    cpusubtype CPU_SUBTYPE_I386_ALL
    offset 4096
    size 17652
    align 2^12 (4096)
architecture ppc7400
    cputype CPU_TYPE_POWERPC
    cpusubtype CPU_SUBTYPE_POWERPC_7400
    offset 24576
    size 13636
    align 2^12 (4096)
logan /opt/malware/mach-o $
```

Lipo

0xCAFEBABE



## 0x03 – Tools For Analysis (Static)

LIPO

```
logan /opt/malware/mach-o $ lipo -info sample  
Architectures in the fat file: sample are: armv7 armv7s  
logan /opt/malware/mach-o $  
logan /opt/malware/mach-o $  
logan /opt/malware/mach-o $ lipo -info sample_10  
Architectures in the fat file: sample_10 are: i386 ppc7400  
logan /opt/malware/mach-o $
```

```
logan /opt/malware/mach-o $  
logan /opt/malware/mach-o $ lipo -extract i386 -output sample10_i386 sample_10  
logan /opt/malware/mach-o $  
logan /opt/malware/mach-o $ file sample10_i386  
sample10_i386: Mach-O universal binary with 1 architecture  
sample10_i386 (for architecture i386): Mach-O executable i386  
logan /opt/malware/mach-o $
```



# 0x03 – Tools For Analysis (Static)

OTool

```
logan /opt/malware/mach-o $ otool -f sample
Fat headers
fat_magic 0xcafebabe
nfat_arch 2
architecture 0
    cputype 12
    cpusubtype 9
    capabilities 0x0
    offset 16384
    size 57824
    align 2^14 (16384)
architecture 1
    cputype 12
    cpusubtype 11
    capabilities 0x0
    offset 81920
    size 57824
    align 2^14 (16384)
logan /opt/malware/mach-o $ otool -f sample10_i386
Fat headers
fat_magic 0xcafebabe
nfat_arch 1
architecture 0
    cputype 7
    cpusubtype 3
    capabilities 0x0
    offset 4096
    size 17652
    align 2^12 (4096)
```



# 0x03 – Tools For Analysis (Static)

```
logan /opt/malware/mach-o $ nm sample
```

```
sample (for architecture armv7):
```

```
0000b744 s stub_helpers
0000bef0 s __.str3
    U __CFDataGetBytePtr
    U __CFDataGetLength
    U __CFDataGetTypeID
    U __CFGetTypeID
    U __CFURLCreateStringByAddingPercentEscapes
    U __IOMasterPort
    U __IORRegistryEntrySearchCFProperty
    U __IORRegistryGetRootEntry
    U __NSLog
0000c4d0 S __NXArgc
0000c4d4 S __NXArgv
0000c120 s __OBJC_$_CLASS_METHODS__ARCLite__
    U __OBJC_CLASS_$_NSArray
    U __OBJC_CLASS_$_NSAutoreleasePool
    U __OBJC_CLASS_$_NSBundle
    U __OBJC_CLASS_$_NSDictionary
    U __OBJC_CLASS_$_NSMutableArray
    U __OBJC_CLASS_$_NSMutableDictionary
    U __OBJC_CLASS_$_NSMutableOrderedSet
    U __OBJC_CLASS_$_NSMutableString
    U __OBJC_CLASS_$_NSMutableURLRequest
    U __OBJC_CLASS_$_NSOrderedSet
    U __OBJC_CLASS_$_NSString
    U __OBJC_CLASS_$_NSURL
    U __OBJC_CLASS_$_NSURLConnection
0000c274 s __OBJC_CLASS_$_ARCLite__
0000c0d0 s __OBJC_CLASS_RO_$_ARCLite__
0000c288 s __OBJC_METACLASS_$_ARCLite__
0000c0f8 s __OBJC_METACLASS_RO_$_ARCLite__
    U __Block_copy
```

NM



# 0x03 – Tools For Analysis (Static)

CODESIGN

```
logan /opt/malware/mach-o $ codesign -dvvv sample_07
Executable=/opt/malware/mach-o/sample_07
Identifier=com.maiyadi.start
Format=Mach-O universal (armv7 armv7s)
CodeDirectory v=20100 size=466 flags=0x0(none) hashes=15+5 location=embedded
Hash type=sha1 size=20
CDHash=11e74087e067823ed346173aa4a6f96152bf0abc
Signature size=4319
Authority=iPhone Developer: li tjcy (967X86AAT5)
Authority=Apple Worldwide Developer Relations Certification Authority
Authority=Apple Root CA
Signed Time=May 6, 2014, 12:06:50 AM
Info.plist=not bound
TeamIdentifier=not set
Sealed Resources=none
Internal requirements count=1 size=176
logan /opt/malware/mach-o $
```



# 0x03 – Tools For Analysis (Static)

MachOView

MachOView File Edit Format View Window Help

sample\_01

RAW RVA

Search

Offset Data Description Value

Offset	Data	Description	Value
00000000	BEBAFEC A	Magic Number	FAT_CIGAM
00000004	03000000	Number of Architecture	3
00000008	07000001	CPU Type	CPU_TYPE_X86_64
0000000C	03000080	CPU SubType	CPU_SUBTYPE_X86_64_ALL
00000010	00100000	Offset	4096
00000014	F0420000	Size	17136
00000018	0C000000	Align	4096
0000001C	07000000	CPU Type	CPU_TYPE_I386
00000020	03000000	CPU SubType	CPU_SUBTYPE_I386_ALL
00000024	00600000	Offset	24576
00000028	88410000	Size	16776
0000002C	0C000000	Align	4096
00000030	12000000	CPU Type	CPU_TYPE_POWERPC
00000034	0A000000	CPU SubType	CPU_SUBTYPE_POWERPC_7400
00000038	00B00000	Offset	45056
0000003C	AC500000	Size	20652
00000040	0C000000	Align	4096

Fat Binary

Fat Header

Executable (X86\_64) [SDK10.6]

- Mach64 Header
- Load Commands
- Section64 (\_TEXT, \_text)
- Section64 (\_TEXT, \_symb...)
- Section64 (\_TEXT, \_cstring)
- Section64 (\_TEXT, \_const)
- Section64 (\_TEXT, \_stub...)
- Section64 (\_TEXT, \_unwind)
- Section64 (\_TEXT, \_eh\_frame)
- Section64 (\_DATA, \_program)
- Section64 (\_DATA, \_mod\_info)
- Section64 (\_DATA, \_nl\_symbols)
- Section64 (\_DATA, \_la\_symbols)
- Section64 (\_DATA, \_data)
- Dynamic Loader Info
- Symbol Table
- Dynamic Symbol Table
- String Table

Executable (X86) [SDK10.6 Ta...]

Executable (PPC)



# 0x03 – Tools For Analysis (Static)

HOPPER

Hopper Disassembler v3

File Edit Find Modify Navigate Debug Scripts Window Help

sample10\_i386.hop

Labels Strings

Q~Search Tag Scope

start dyld\_stub\_binding\_helper \_\_dyld\_func\_lookup \_\_init\_daemon \_encryptFile \_copyfile \_main \_\_\_progname \_environ \_NXArgv \_NXArgc RC4 RC4\_set\_key access chdir chmod\$UNIX2003 close\$UNIX2003 exit fclose fopen fork fread free fwrite\$UNIX2003 malloc memset

0000174b hlt  
dyld\_stub\_binding\_helper:  
call 0x1751  
pop eax  
push dword [ds:eax+0x8bf]  
mov eax, dword [ds:eax+0x8c3]  
jmp eax  
\_\_dyld\_func\_lookup:  
call 0x1765  
pop eax  
mov eax, dword [ds:eax+0xb3]  
jmp eax

===== BEGINNING OF PROCEDURE

\_init\_daemon:  
push ebp  
mov ebp, esp  
push ebx  
sub esp, 0x14  
call imp\_\_jump\_table\_fork  
test eax, eax  
jne 0x178e

call imp\_\_jump\_table\_setsid  
xor ebx, ebx  
call imp\_\_jump\_table\_fork  
test eax, eax  
je 0x179a

> analysis section \_\_dyld  
> analysis segment \_\_OBJC  
> analysis section \_\_image\_info  
> analysis segment \_\_IMPORT  
> analysis section \_\_jump\_table  
> analysis segment \_\_LINKEDIT  
> analysis segment External Symbols  
Background analysis ended

Address 0x176e, Segment TEXT, \_\_init\_daemon + 0, Section text, file offset 0x76e



# 0x03 – Tools For Analysis (Static)

CLASS-DUMP

```
logan /opt/malware/mach-o $ class-dump sample
1. Infected (bash)

// Generated by class-dump 3.5 (64 bit).
// class-dump is Copyright (C) 1997-1998, 2000-2001, 2004-2013 by Steve Nygard.

#pragma mark -

// File: sample
// UUID: 4D44DD86-BAF1-30F6-983E-9E11EA45F07D
// Arch: armv7
// Minimum iOS version: 4.3.0
// SDK version: 7.1.0

// Objective-C Garbage Collection: Unsupported
//

@protocol __ARCLiteIndexedSubscripting__
- (void)setObject:(id)arg1 atIndexedSubscript:(unsigned int)arg2;
- (id)objectAtIndexedSubscript:(unsigned int)arg1;
@end

@protocol __ARCLiteKeyedSubscripting__
- (void)setObject:(id)arg1 forKeyedSubscript:(id)arg2;
- (id)objectForKeyedSubscript:(id)arg1;
@end

logan /opt/malware/mach-o $
```



## 0x03 – Tools For Analysis (Dynamic)

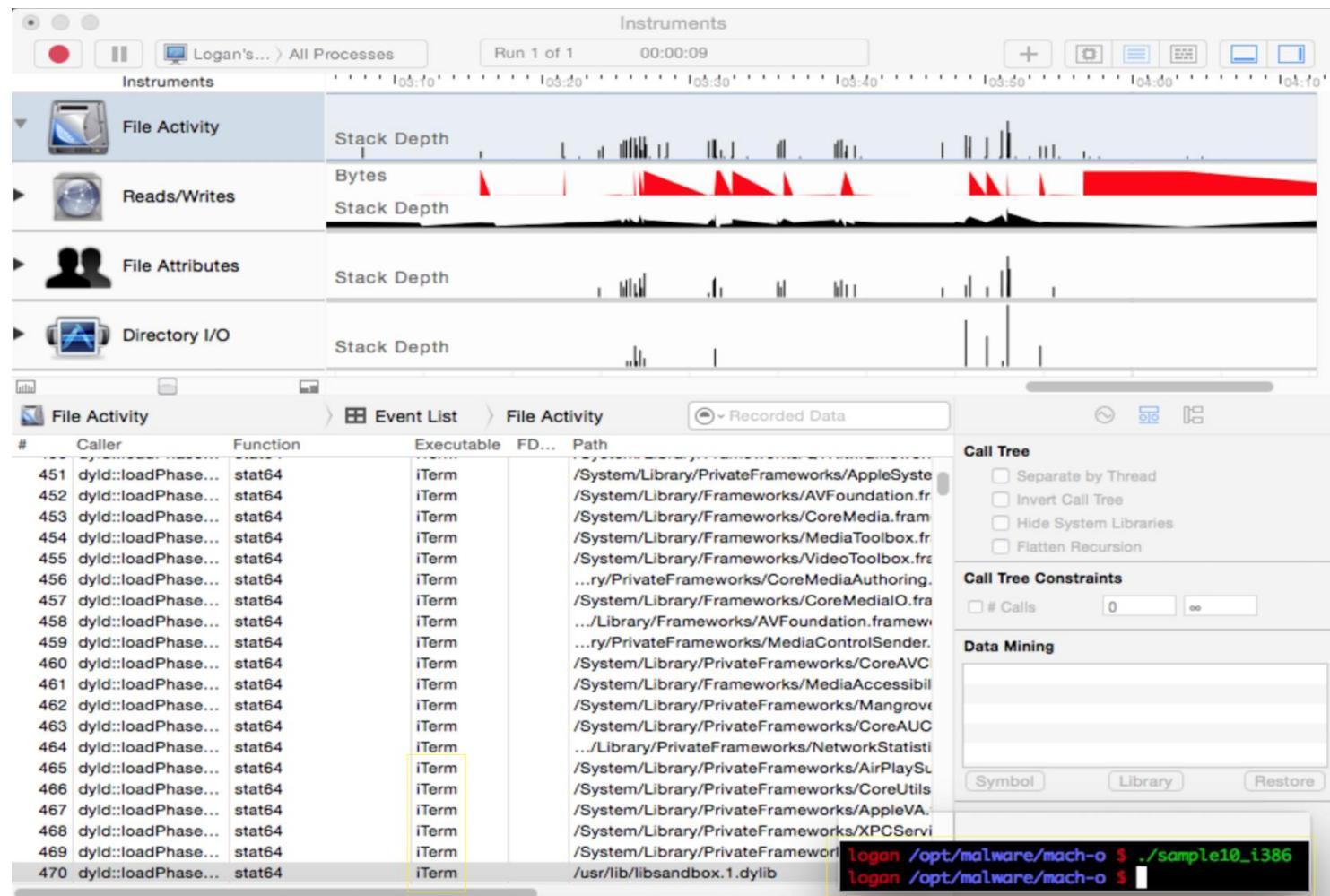
### VMWARE FUSION / PARALLELS / VIRTUALBOX

- Keep Virtualization Software Updated
- Use System Tools Installed in VM
- Network Host-Only mode
- If you use Shared Folder(Host) leave it as “read-only”
- Disable Gatekeeper (Allow apps downloaded from: Anywhere)



# 0x03 – Tools For Analysis (Dynamic)

XCODE





# 0x03 – Tools For Analysis (Dynamic)

IDA PRO

also is a static tool

The screenshot shows the IDA Pro interface with the following windows:

- Functions window:** Lists functions including `__static_initialization_and_destruction_0(int,int)`, `global constructor keyed to '_wr_buf'`, `start`, `TaskStop(void)`, `BasePostBuffer(char *,char *,char *,int)`, `GetHttpFileSize(void)`, and `TaskStart(void)`.
- IDA View A:** Shows assembly code for the `__static_initialization_and_destruction_0(int,int)` function:

```
; Attributes: bp-based frame
; __static_initialization_and_destruction_0(int, int)
_Z41__static_initialization_and_destruction_0ii proc near
push ebp
mov ebp, esp
sub esp, 18h
dec eax
jnz short locret_1982
```
- Hex View A:** Shows the hex dump of the assembly code.
- Structures, Enums, Imports, Exports:** Standard IDA Pro navigation tabs.
- Graph overview:** A call graph showing the control flow between functions.
- Output window:** Displays logs and messages from the IDA Pro process, including the compilation of idc files and the execution of the main function.
- Python:** A Python console window.



# 0x03 – Tools For Analysis (Dynamic)

LLDB

```
logan ~/Desktop/lab_sample $  
logan ~/Desktop/lab_sample $ lldb sample  
(lldb) target create "sample"  
Current executable set to 'sample' (armv7).  
(lldb) disassemble --name main  
sample`main:  
sample[0xacac] <+0>: push {r4, r5, r6, r7, lr}  
sample[0xacae] <+2>: add r7, sp, #0xc  
sample[0xacb0] <+4>: push.w {r8, r10, r11}  
sample[0xacb4] <+8>: sub sp, #0x20  
sample[0xacb6] <+10>: movw r0, #0x14be  
sample[0xacba] <+14>: movt r0, #0x0  
sample[0xacbe] <+18>: movw r2, #0x158c  
sample[0xaccc2] <+22>: movt r2, #0x0  
sample[0xaccc6] <+26>: add r0, pc  
sample[0xaccc8] <+28>: add r2, pc  
sample[0xacca] <+30>: ldr r1, [r0]  
sample[0xaccc] <+32>: ldr r0, [r2]  
sample[0xacce] <+34>: blx 0xbfa8 ; symbol stub for: objc_msgSend  
sample[0xacd2] <+38>: movw r1, #0x14b6  
sample[0acd6] <+42>: movt r1, #0x0  
sample[0xacda] <+46>: add r1, pc  
sample[0xacdc] <+48>: ldr r1, [r1]  
sample[0xacde] <+50>: blx 0xbfa8 ; symbol stub for: objc_msgSend  
sample[0xae2] <+54>: str r0, [sp, #0x1c]  
sample[0xae4] <+56>: movw r0, #0x14ec  
sample[0xae8] <+60>: movt r0, #0x0  
sample[0xaeec] <+64>: movw r2, #0x1562  
sample[0xacf0] <+68>: movt r2, #0x0  
sample[0acf4] <+72>: add r0, pc  
sample[0acf6] <+74>: add r2, pc  
sample[0acf8] <+76>: ldr r1, [r0]  
sample[0xacfa] <+78>: ldr r0, [r2]  
sample[0acf0c] <+80>: mov r5, r2  
sample[0acf0e] <+82>: str r1, [sp, #0x8]  
sample[0xad00] <+84>: mov r8, r1  
sample[0xad02] <+86>: blx 0xbfa8 ; symbol stub for: objc_msgSend  
sample[0xad06] <+90>: mov r7, r7
```



# 0x03 – Tools For Analysis (Dynamic)

FSEVENTER

The screenshot shows the fseventer application interface. At the top, there's a menu bar with Apple, fseventer, File, Edit, Window, Help. The title bar says "fseventer - Stopped". On the right, there are icons for information, printer, file, and other tools. Below the menu is a toolbar with various icons. The main area displays a file system tree. A yellow box highlights a folder named "sample\_03" under "/private/tmp/CurlUpload/2A303B77-AB". Inside this folder are several files: "checkvir.plist", "checkvir", "com.apple.spaces.plist", "com.apple.spaces.plist.t9kyHoV", "com.fernlightning.fseventer.plist", and "com.fernlightning.fseventer.plist.BeYAcAv". To the right of the tree, there are two red crossed-out entries: "app.com.fernlightning.fseventer.playlist" and "app.com.fernlightning.fseventer.playlist.Kus4Bm". At the bottom, a terminal window shows the command "logon /opt/malware/mach-o \$ ./sample\_03" followed by the output "user=logon", "file name is :./sample\_03", and "ret = 6 (write\_error = 0)".



# 0x03 – Tools For Analysis (Dynamic)

OPEN SNOOP

TIME	STRTIME	UID	PID	FD	ERR	PATH	ARGS
1684253508	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app Dock\0	
1684253612	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app/Contents Dock\0	
1684253685	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app/Contents/Info.plist Dock\0	
1684253881	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app Dock\0	
1684253941	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app/Contents Dock\0	
1684253992	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app/Contents/Info.plist Dock\0	
1684255714	2015 Apr 22 04:23:11	501	196	35	0	/Applications/0xED.app/Contents/PkgInfo Dock\0	
1684256230	2015 Apr 22 04:23:11	501	196	35	0	/Library/Caches/com.apple.iconservices.store/69650B76-3F59-9236-55Df-98891864DFB3.isdata Dock\0	
1684619763	2015 Apr 22 04:23:12	501	2507	3	0	/dev/dtracehelper sh\0	
1684621266	2015 Apr 22 04:23:12	501	2507	-1	6	/dev/tty sh\0	
1684625346	2015 Apr 22 04:23:12	501	2509	3	0	/dev/dtracehelper grep\0	
1684625619	2015 Apr 22 04:23:12	501	190	4	0	/Users/logan/Library/Preferences/com.apple.spaces.plist.MPIBvC1 cfprefsd\0	
1684624901	2015 Apr 22 04:23:12	501	190	4	0	/Users/logan/Library/Preferences/ByHost/com.apple.loginwindow.564D4EC2-D722-B7E0-9098-4A8FA55B4CBE.plist.FFaj8zs cfprefsd\0	
1684624821	2015 Apr 22 04:23:12	501	2508	3	0	/dev/dtracehelper ps\0	
1684656366	2015 Apr 22 04:23:12	501	2510	3	0	/dev/dtracehelper sh\0	
1684674588	2015 Apr 22 04:23:12	501	2512	3	0	/dev/dtracehelper grep\0	
1684672404	2015 Apr 22 04:23:12	501	2510	-1	6	/dev/tty sh\0	
1684674195	2015 Apr 22 04:23:12	501	2511	3	0	/dev/dtracehelper ps\0	
1685058001	2015 Apr 22 04:23:12	0	30	5	0	/var/db/BootCaches/2A303B77-AB26-435A-BBDA-3762B26E04E5/app.com.suvatech.0xED.playlist.2IzoWq warmd\0	
1685428714	2015 Apr 22 04:23:13	501	2513	3	0	/dev/dtracehelper lssave\0	
1685439436	2015 Apr 22 04:23:13	501	2513	4	0	/var/folders/58/r3pxxb4s1nnfyt6xjb4vh4wm0000gn/0//com.apple.LaunchServices-103501.csstore~ lssave\0	
1685435681	2015 Apr 22 04:23:13	501	2513	3	0	/dev/autofs_nowait lssave\0	
1685435708	2015 Apr 22 04:23:13	501	2513	4	0	/Users/logan/.CFUserTextEncoding lssave\0	
1685436099	2015 Apr 22 04:23:13	501	2513	3	0	/dev/autofs_nowait lssave\0	
1685436110	2015 Apr 22 04:23:13	501	2513	4	0	/Users/logan/.CFUserTextEncoding lssave\0	
1685434581	2015 Apr 22 04:23:13	501	2513	-1	2	/etc/.mdns_debug lssave\0	



# 0x03 – Tools For Analysis (Dynamic)

ACTIVITY MONITOR

Activity Monitor

File Edit View Window Help

Activity Monitor (My Processes)

Process Name	% CPU	CPU Time	Threads	Idle Wake Ups	PID	User
Activity Monitor	2.7	1.46	6	3	16352	logan
iTerm	1.4	1.14	8	3	16354	logan
Dock	0.1	7.38	5	0	196	logan
Spotlight	0.1	4.10	6	0	206	logan
diagnostics_agent	0.1	0.48	4	0	267	logan
loginwindow	0.1	5.75	4	0	65	logan
distnoted	0.1	2.93	8	0	188	logan
sample_03	0.0	0.04	2	2	16318	logan
pkd	0.0	0.40	4	0	220	logan
nsurlstoraged	0.0	0.87	4	0	237	logan
sample_03	0.0	0.01	2	1	16369	logan
cfprefsd	0.0	4.11	4	0	190	logan
fontd	0.0	2.63	3	0	209	logan
bird	0.0	0.21	4	0	217	logan
com.apple.CoreSimulator.C...	0.0	0.13	5	0	16179	logan
iconservicesagent	0.0	0.30	4	0	229	logan
LaterAgent	0.0	0.60	3	0	288	logan
CalNCSERVICE	0.0	0.30	2	0	239	logan
imagent	0.0	0.27	2	0	242	logan
CallHistorySyncHelper	0.0	0.25	2	0	245	logan
Finder	0.0	47.51	3	0	199	logan
cloudd	0.0	1.95	2	0	248	logan
pbs	0.0	0.22	2	0	251	logan

System: 1.74% CPU LOAD User: 3.01% Threads: 642 Idle: 95.25% Processes: 169



# 0x03 – Tools For Analysis (Dynamic)

PROCXP

1. Infected (procexp.universa)																		
PID	PPID	UID	TTY	COMMAND	PRI	#TH	VSS	RSS	S	STIME	TIME	CPU	FDs	Net RX	Net TX			
731	1	501	none	QuickLookSatell	4	2	2425M	7672K	S	04:59:23	00.16	0	4	---	---			
730	1	501	none	quicklookd	4	7	12929M	10M	S	04:59:23	00.20	0	21	---	---			
729	1	501	none	mdworker	4	3	12430M	7832K	S	04:59:21	00.04	0	5	---	---			
726	1	501	none	syncdefaultsd	31	2	12422M	13M	S	04:59:08	00.12	0	4	---	---			
725	296	501	268435	procexp.univers	31	4/1	12443M	45M	R	04:59:06	00.84	48	5	0B	0B			
578	1	501	none	helpd	4	2	12422M	5416K	S	03:18:58	00.03	0	4	---	---			
456	1	501	none	USBAgent	31	2	12400M	5276K	S	02:27:12	00.03	0	4	---	---			
417	1	501	none	nbagent														
365	1	501	none	mdflagwriter														
345	1	501	none	EscrowSecurity														
313	1	501	none	storedownloadd														
312	1	501	none	LaterAgent														
311	1	501	none	storeassett														
310	1	501	none	storelegacy														
296	295	501	268435	bash														
292	1	501	none	CoreServicesUL														
285	1	501	none	com.apple.Inpu														
283	1	501	none	iTerm														
281	1	501	none	AppleSpell														
280	1	501	none	pbs														
275	1	501	none	com.apple.noti														
273	1	501	none	com.apple.meta														
272	1	501	none	CalNCServic														

1. Infected (procexp.universa)

Process: 723 Name: syncdefaultsd Parent: 1 Status: runnable

Flags: 64-bit,called exec,Adaptive,Important,Donor

UID: 501 RUID: 501 SVUID: 501

GID: 20 RGID: 20 SVGID: 20

Virtual size: 2422M (2540539904) Resident size: 13M (14589952)

Time: 00.11 = 00.09 (User) + 00.02 (System)

Syscalls: 3427 Mach Traps: 1571

Disk I/O: Read OK Written: 60K

No Network I/O detected for this process

#Threads: 2 (Process has no workqueues)  
(press T to display Thread Information)

Process Hierarchy:  
723 syncdefaultsd has no children

4 File descriptors: 3 files (press F for detailed information)



## 0x03 – Tools For Analysis (Dynamic)

TCPDUMP

```
loganbr ~ $ tcpdump -i en0 -w lab_infected.pcap
tcpdump: listening on en0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C101 packets captured
102 packets received by filter
0 packets dropped by kernel
loganbr ~ $ 
loganbr::Zion-Logan-2::          0:bash*
```



# 0x03 – Tools For Analysis (Dynamic)

COCOA

lab\_infected.pcap

Select a filter predicate

Filter

Id	Source	Destination	Captured Length	Packet Length	Protocol	Date Received	Time Delta	Information
32	172.16.1.243	146.255.36.1	66	66	TCP	2015-05-03 16:20:26.131	4.607989	56980 -> HTTP ([ACK, FIN], Seq=2041904939, Ack=86042694...
33	172.16.1.243	8.8.8.8	77	77	UDP	2015-05-03 16:20:26.298	4.775345	49245 > DOMAIN
34	146.255.36.1	172.16.1.243	66	66	TCP	2015-05-03 16:20:26.349	4.826088	HTTP -> 56980 ([ACK, FIN], Seq=860426947, Ack=204190494...
35	172.16.1.243	146.255.36.1	66	66	TCP	2015-05-03 16:20:26.349	4.826150	56980 -> HTTP ([ACK], Seq=2041904940, Ack=860426948, Wi...
36	8.8.8.8	172.16.1.243	179	179	UDP	2015-05-03 16:20:26.459	4.935370	DOMAIN > 49245
37	172.16.1.243	146.255.36.1	78	78	TCP	2015-05-03 16:20:29.484	7.960776	56981 -> HTTP ([SYN], Seq=1784175861, Ack=0, Win=65535)
38	172.16.1.243	255.255.255.255	167	167	UDP	2015-05-03 16:20:29.714	8.190599	17500 > 17500
39	172.16.1.243	172.16.1.255	167	167	UDP	2015-05-03 16:20:29.714	8.190769	17500 > 17500
40	146.255.36.1	172.16.1.243	74	74	TCP	2015-05-03 16:20:29.715	8.192112	HTTP -> 56981 ([ACK, SYN], Seq=3313510592, Ack=1784175...
41	172.16.1.243	146.255.36.1	66	66	TCP	2015-05-03 16:20:29.715	8.192154	56981 -> HTTP ([ACK], Seq=1784175862, Ack=3313510593,...
42	172.16.1.243	146.255.36.1	145	145	TCP	2015-05-03 16:20:29.715	8.192326	56981 -> HTTP ([ACK, PUSH], Seq=1784175862, Ack=331351...
43	172.16.1.243	213.199.179.168	77	77	UDP	2015-05-03 16:20:30.121	8.598231	57757 > 40008

Details Values

Packet

- ID 42
- Date received 2015-05-03 16:20:29.715 (-0300)
- Time since first p... 8.192326 seconds
- Packet length 145 bytes
- Captured length 145 bytes

Ethernet-Header

- Source 60:03:08:9f:01:38
- Destination b8:c7:5d:cd:ed:d6
- Type IP (0x0800)

IP-Header

- Length 20 bytes
- Version 4
- Differentiated Se... 0x00
- Total length 131 bytes
- Identification 0xd711 (55057)

000: B8 C7 5D CD ED D6 60 03 08 9F 01 38 08 00 45 00 00 83 D7 11 40 00 40 06 FE 5F AC 10 01 F3 92 FF 24 01 DE 95 00 ..]....`....8.E.....@.0.....\$....  
037: 50 6A 58 5C F6 C5 80 28 C1 80 18 10 08 6B 5E 00 00 01 01 08 0A 36 2C E5 AC C5 AB 1F DC 47 45 54 20 2F 70 6C 61 PjX\...C.....k^.....6,.....GET /pla  
074: 69 6E 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 63 75 72 6C 2F 37 2E 33 38 2E 30 0D in HTTP/1.1..User-Agent: curl/7.38.0.  
111: 0A 48 6F 73 74 3A 20 69 70 65 63 68 6F ZE 6E 65 74 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 0D 0A .Host: ipecho.net..Accept: \*/....

Fileformat: 2.4 Snaplength: 65535 bytes Linktype: ETHERNET (DLT\_EN10MB) Filesize: 15033 bytes Packets: 101 of 101 (1 selected)



# 0x03 – Tools For Analysis (Dynamic)

WIRESHARK

Screenshot of Wireshark showing network traffic analysis. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), toolbar, and a list of captured packets.

The list of packets shows various interactions, including:

- HTTP requests to 172.16.1.243 and 146.255.36.1.
- TCP connections between 172.16.1.243 and 146.255.36.1.
- DNS queries and responses.
- UDP traffic from 172.16.1.243 to 213.199.179.168.
- Dropbox LAN sync Discovery Protocol traffic.
- Internet Protocol Version 4 (IPv4) traffic.
- Transmission Control Protocol (TCP) traffic.
- Hypertext Transfer Protocol (HTTP) traffic, including a full request to `http://ipecho.net/plain`.

The bottom pane displays the raw hex and ASCII data of a selected frame (Frame 145).

```
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Apple_9f:01:38 (60:03:08:9f:01:38), Dst: Apple_cd:ed:d6 (b8:c7:5d:cd:ed:d6)
  Destination: Apple_cd:ed:d6 (b8:c7:5d:cd:ed:d6)
  Source: Apple_9f:01:38 (60:03:08:9f:01:38)
  Type: IP (0x0800)
  Internet Protocol Version 4, Src: 172.16.1.243 (172.16.1.243), Dst: 146.255.36.1 (146.255.36.1)
  Transmission Control Protocol, Src Port: 56981 (56981), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 79
  Hypertext Transfer Protocol
    GET /plain HTTP/1.1\r\n
    User-Agent: curl/7.38.0\r\n
    Host: ipecho.net\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://ipecho.net/plain]
    [HTTP request 1/1]
    [Response in frame: 50]
```

Frame (frame), 145 bytes | Packets: 101 · Displayed: 101 (100%) · Load time: 0:00:000 | Profile: Default



# 0x03 – Tools For Analysis (Dynamic)

LSOCK

Time	Local Addr	Remote Addr	If	State	P
11:18:52	0.0.0.0:23945	*.*	0	N/A	1
11:18:52	fe80::20c:29ff:fe5b:4cbe:123	*.*	4	N/A	
11:18:52	fe80::1:123	*.*	1	N/A	7
11:18:52	127.0.0.1:123	*.*	1	N/A	7
11:18:52	::1:123	*.*	1	N/A	7
11:18:52	::123	*.*	0	N/A	7
11:18:52	0.0.0.0:123	*.*	0	N/A	7
11:18:52	0.0.0.0:0	*.*	0	N/A	5
11:18:52	0.0.0.0:0	*.*	0	N/A	1
11:18:52	::5353	*.*	1	N/A	4
11:18:52	0.0.0.0:5353	*.*	1	N/A	4
11:18:52	::0	*.*	0	N/A	4
11:18:52	0.0.0.0:0	*.*	0	N/A	4
11:18:52	::0	*.*	0	N/A	2
11:18:52	0.0.0.0:137	*.*	0	N/A	1
11:18:52	0.0.0.0:138	*.*	0	N/A	1
11:18:52	::1:7026	::1:49328	1	ESTABLISHED	9
11:18:52	::1:49328	::1:7026	1	ESTABLISHED	9
11:18:52	::1:7026	::1:49327	1	ESTABLISHED	9
11:18:52	::1:49327	::1:7026	1	ESTABLISHED	9
11:20:15	0.0.0.0:0	*.*	0	N/A	4
11:20:15	::5353	*.*	0	N/A	4
11:20:16	172.16.249.144:49330	201.6.16.157:443	4	SYN_SENT	9
11:20:16	0.0.0.0:0	*.*	0	CLOSED	9
11:20:16	0.0.0.0:0	*.*	0	CLOSED	9
11:20:16	172.16.249.144:49333	201.6.16.177:80	4	CLOSED	9
11:20:16	0.0.0.0:49334	*.*	0	CLOSED	9
11:20:16	0.0.0.0:49335	*.*	0	CLOSED	9
11:20:17	172.16.249.144:123	*.*	4	N/A	7
11:20:20	172.16.249.144:49337	64.233.186.95:443	4	CLOSED	9
11:20:20	0.0.0.0:0	*.*	0	CLOSED	9
11:20:20	0.0.0.0:0	*.*	0	CLOSED	9
11:20:21	172.16.249.144:49340	173.194.118.62:443	4	SYN_SENT	9



# 0x03 – Tools For Analysis (Dynamic)

Little Snitch Configuration

Prevent Changes Preferences

Search Info

Rules

- All Rules
- Last 24 Hours
- Temporary Rules (29)
- Unapproved Rules (2)
- GUI Applications
- Background Processes
- Protected Rules
- Global Rules
- System Rules
- Incoming Connections

Suggestions

- Login Connections (2)
- Expired Temporary Rules

Profiles

- Effective in all profiles

**locationd**

wants to connect to **gs-loc.apple.com** on port 443 (https)

Forever Once

Any Connection

Only port 443 (https)

Only gs-loc.apple.com

Only gs-loc.apple.com and port 443 (https)

Deny Allow

Little Snitch Network Monitor

Temporary Rules

Google Drive iTunes ocspd Dropbox apsd Stock + com.apple.geod.xpc com.apple.photomoments.xpc com.apple.iCloudHelper.xpc Google Chrome SubmitDiagInfo SystemUIServer syncdefaults cloudd SpotlightNetHelper IMRemoteURLConnectionAgent.xpc nsurlsessiond CalendarAgent locationd UserEventAgent sntp mDNSResponder

talk.i.google.com > 3 more  
a473.phobos.g.aaplimg.com > 9 more  
sr.symcd.com > 3 more  
4.notify.dropbox.com > 2 more  
1-courier.push.apple.com > 1 more  
iphone-wu.apple.com  
gspe21.ls.apple.com  
gspe21.ls.apple.com  
p01-quota.icloud.com > 1 more  
api.shodan.io > 11 more  
radarsubmissions.apple.com  
ip.bjango.com  
p01-keyvalueservice.icloud.com  
p29-ckdatabase.icloud.com > 2 more  
api.smoot.apple.com  
query.ess.apple.com > 2 more  
p29-ckdatabase.icloud.com > 2 more  
p01-caldav.icloud.com  
gs-loc.apple.com  
www.appleiphonecell.com  
time.apple.com  
8.8.8.8

20m



# 0x04 – Current Threats

ClamXav

Start Scan Stop Pause Update Definitions Open Scan Log Open Update Log Preferences

Source List	Filename	Infection Name	Status
logan	sample_01	Osx.Trojan.Imuler-3	
Documents	sample_02	Osx.Trojan.Imuler-3	
Desktop	sample_03	Osx.Trojan.Imuler-2	
sample_01	sample_04	Osx.Trojan.Lamzev	
sample_01	sample_05	OSX.Trojan.Wirelurker-1	
sample_01.idb	sample_06	Ios.Trojan.Wirelurker	
sample_02	sample_07	OSX.Trojan.Wirelurker-1	
sample_03	sample_08	Osx.Trojan.Imuler-4	
sample_03	sample_09	Osx.Trojan.Imuler-4	
sample_04	sample_10	Osx.Trojan.Imuler-4	

Starting scan...

----- SUMMARY -----  
ClamXav Version: 2.7.5  
Engine Version: 0.98.6  
Scanned Files: 11  
Infected Files: 10

One or more infected files were found, but were left where they are. You can either deal with them yourself, or scan again with the preferences set to move them into a different folder.

+ - ||| Scan Complete



## 0x04 – Current Threats



SHA256: 27989189a16e2eeeca12588c78df8932d5e22416d9b0acb89b58e5ab070c30ffc

Nome do arquivo: 95268cc9dff1812c27f80f7b044a08695c976cb3\_uploadermodule

Taxa de detecção: 32 / 56

Data da análise: 2015-04-20 02:54:09 UTC (1 dia, 11 horas atrás)



Antivírus	Resultado	Atualização
AVG	BackDoor.Generic_c.FCZ	20150420
Ad-Aware	MAC.OSX.Backdoor.Imuler.B	20150420
AhnLab-V3	OSX64-Trojan/Imuleruploader	20150419
Avast	MacOS:Imuler-J [Trj]	20150419
Avira	MACOS/Imuler.A	20150419
BitDefender	MAC.OSX.Backdoor.Imuler.B	20150420
CAT-QuickHeal	Backdoor.MacOSX.Imuler.B	20150418
ClamAV	Osx.Trojan.Imuler-3	20150420
Comodo	UnclassifiedMalware	20150419
DrWeb	Trojan.Muxler.2	20150420

Source: [www.virustotal.com](http://www.virustotal.com)



## 0x04 – Current Threats

### **Mac.BackDoor.OpinionSpy.3**

Names:

MacOS\_X/OpinionSpy.A (Microsoft),  
Mac.BackDoor.OpinionSpy.3 (F-Secure),  
Mac.BackDoor.OpinionSpy.3 (Trend)

.OSA --> ZIP:

- PremierOpinion
- upgrade.xml

Source:

<http://vms.drweb.com/virus/?i=4354056&lng=en>

<http://news.drweb.com/show/?i=9309&lng=en&c=5>



## 0x04 – Current Threats

### **OSX\_KAITEN.A**

**Names:**

MacOS\_X/Tsunami.A (Microsoft),  
OSX/Tsunami (McAfee),  
OSX/Tsunami-Gen (Sophos),  
OSX/Tsunami.A (F-Secure),  
OSX/Tsunami.A (ESET)

**Binary:**

/tmp/.z

**Source:**

[http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/osx\\_kaiten.a](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/osx_kaiten.a)



## 0x04 – Current Threats

### OSX\_CARETO.A

Names:

MacOS:Appetite-A [Trj] (Avast)

OSX/BackDoor.A (AVG)

MAC.OSX.Backdoor.Careto.A (Bitdefender)

OSX/Appetite.A (Eset)

MAC.OSX.Backdoor.Careto.A (FSecure)

Trojan.OSX.Melgato.a (Kaspersky)

OSX/Backdoor-BRE (McAfee)

Backdoor:MacOS\_X/Appetite.A (Microsoft)

OSX/Appetite-A (Sophos)

Source:

[http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/osx\\_careto.a](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/osx_careto.a)



## 0x05 – Conclusions

**Hacking is a way of life**

### Reference:

Sarah Edwards

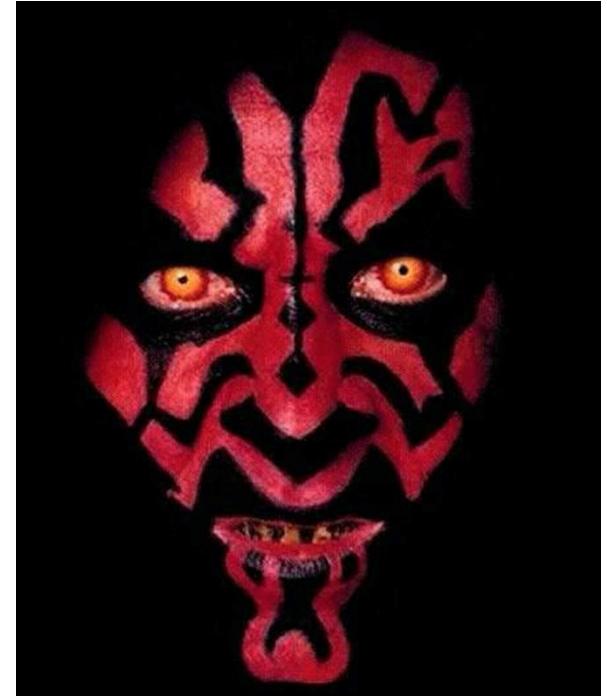
REVERSE Engineering Mac Malware - Defcon 22

<https://www.defcon.org/images/defcon-22/dc-22-presentations/Edwards/DEFCON-22-Sarah-Edwards-Reverse-Engineering-Mac-Malware.pdf>

<https://developer.apple.com/library/mac/documentation/DeveloperTools/Conceptual/MachORuntime/index.html>

[http://www.agner.org/optimize/calling\\_conventions.pdf](http://www.agner.org/optimize/calling_conventions.pdf)

Thanks a Lot  
Any Questions ?



**<http://www.slideshare.net/l0ganbr>**

Contact  
[ricardologanbr@gmail.com](mailto:ricardologanbr@gmail.com)  
@l0ganbr