



MACH-O

UMA NOVA AMEAÇA

Ricardo Amaral a.k.a L0gan



Agenda

0x00 Motivação da Pesquisa

0x01 OS X, O Novo Alvo

0x02 O Formato Mach-O

0x03 Tools - Análise (Estática / Dinâmica)

0x04 Ameaças Atuais

0x05 Conclusão



0x00 - Motivação da Pesquisa

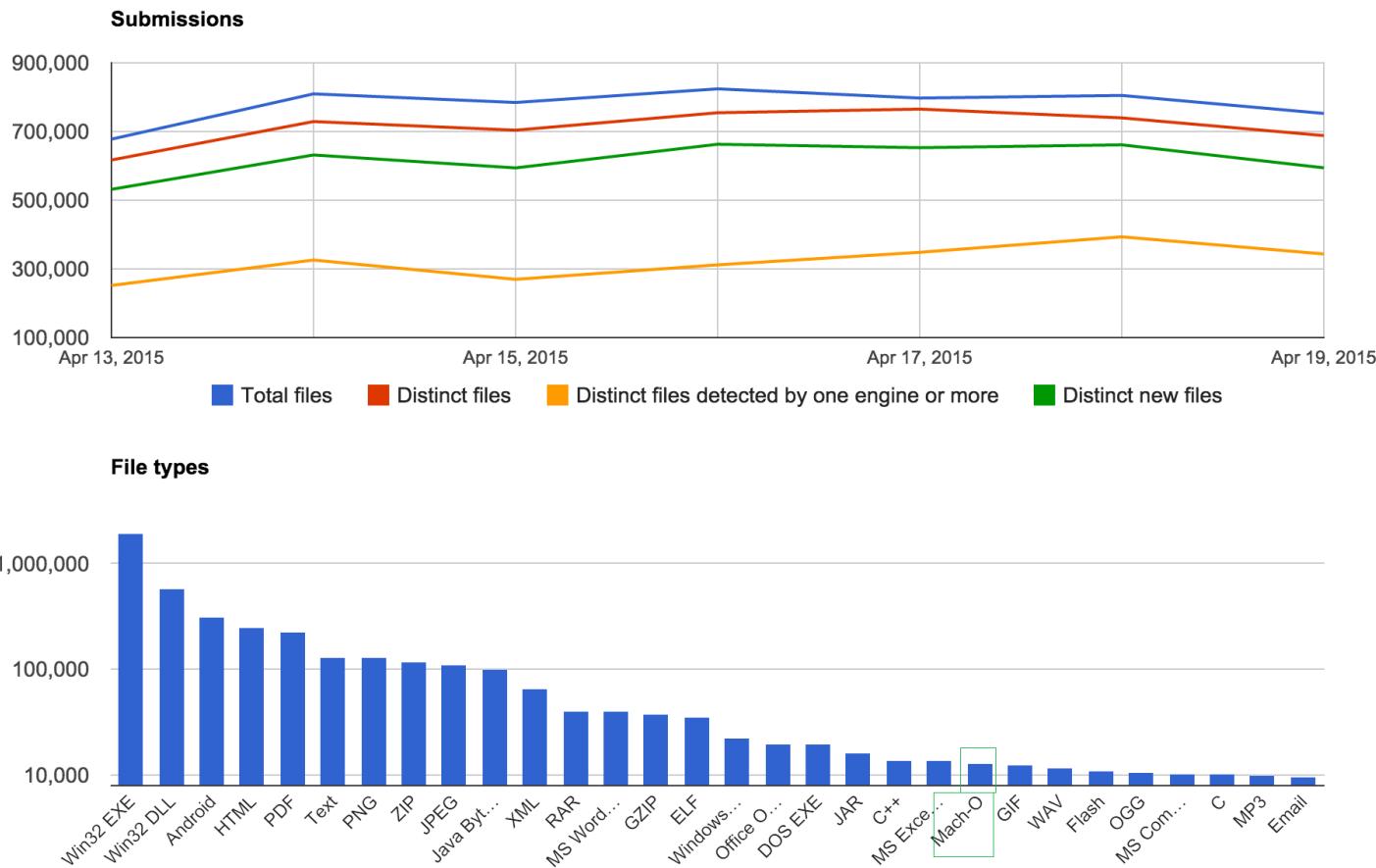
Windows pega vírus !!!

Linux pega vírus?

“Mac não pega vírus”



0x01 – OS X, O Novo Alvo



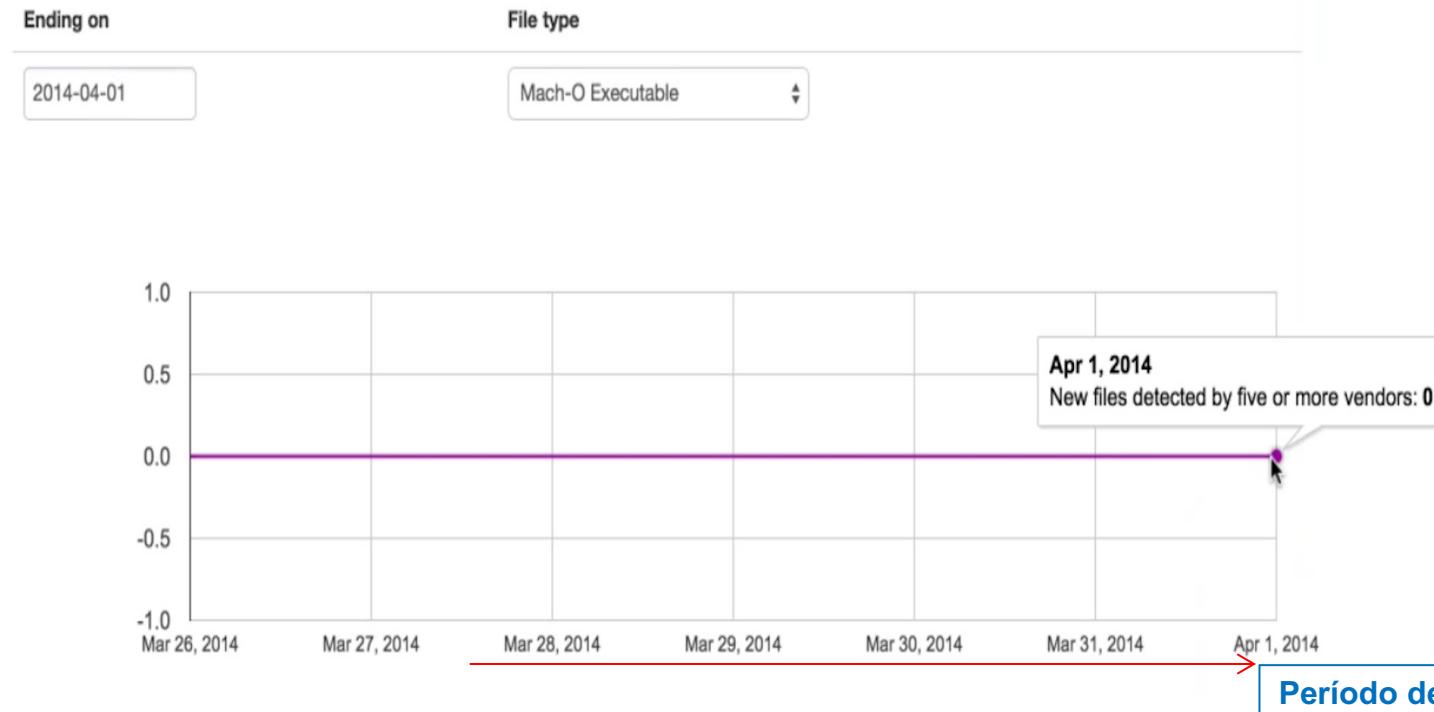
Fonte: www.virustotal.com



0x01 – OS X, O Novo Alvo

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.



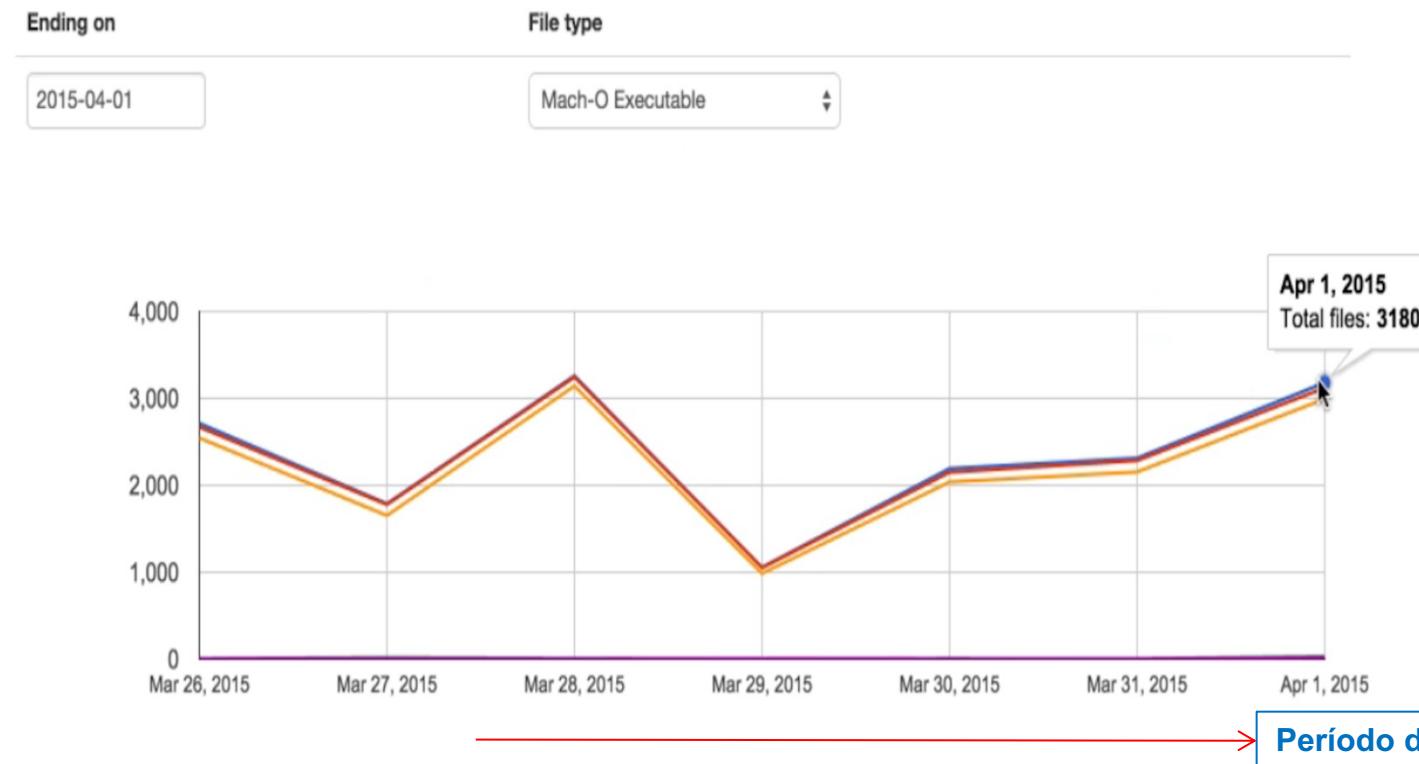
Fonte: www.virustotal.com



0x01 – OS X, O Novo Alvo

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.



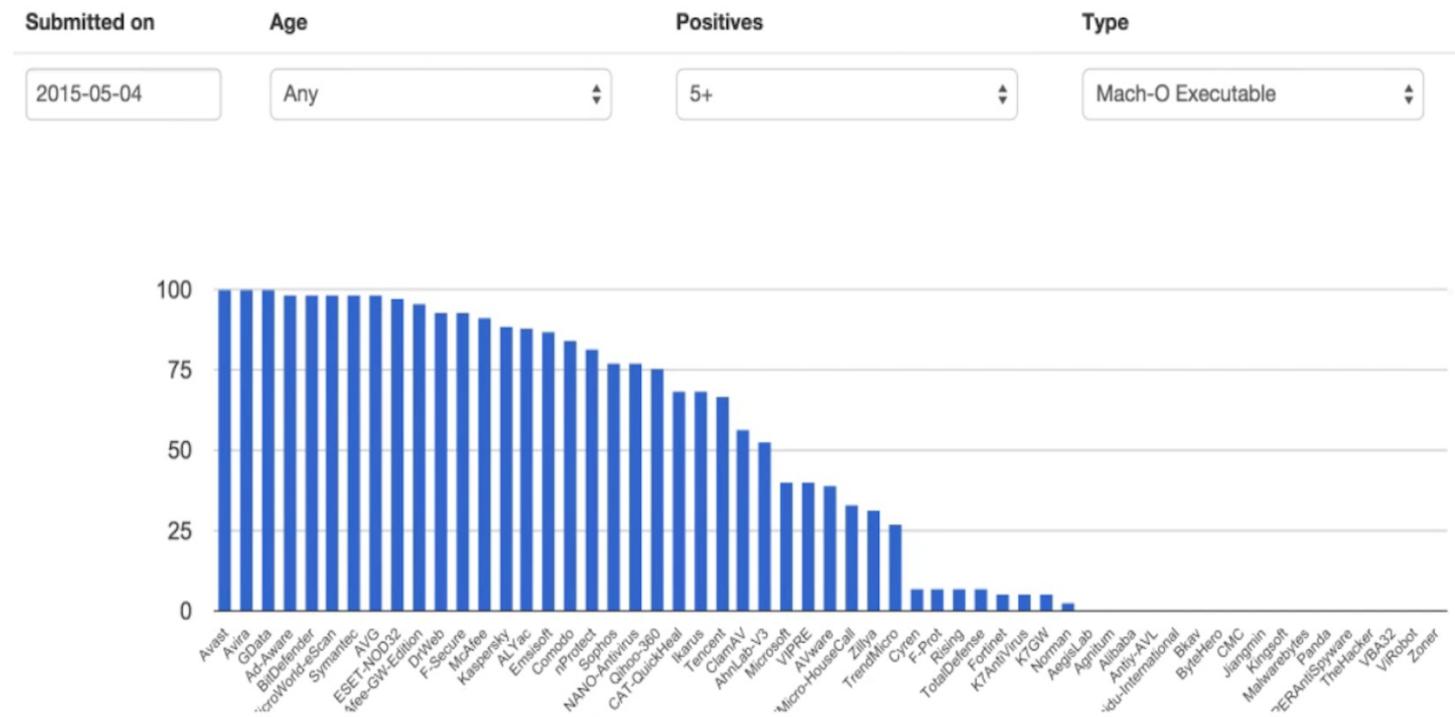
Fonte: www.virustotal.com



0x01 – OS X, O Novo Alvo

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?



Fonte: www.virustotal.com



0x01 – OS X, O Novo Alvo

Sistema operacional da Apple foi a plataforma mais vulnerável de 2014

Por: Renan Lopes

24 de fevereiro de 2015 às 14:06

4297 0



Fonte: <http://gizmodo.uol.com.br/sistema-operacional-da-apple-foi-a-plataforma-mais-vulneravel-de-2014>



0x01 – OS X, O Novo Alvo

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

Fonte: <http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014>



0x02 - O Formato Mach-O

Binário (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 ~ $
```

Binário (Windows)

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

Binário (OS X)

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



0x02 - O Formato Mach-O

O mach-o foi adotado como **padrão** no OS X a partir da versão 10.6.

Atualmente estamos na versão 10.10 (Yosemite).



0x02 - O Formato Mach-O

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)



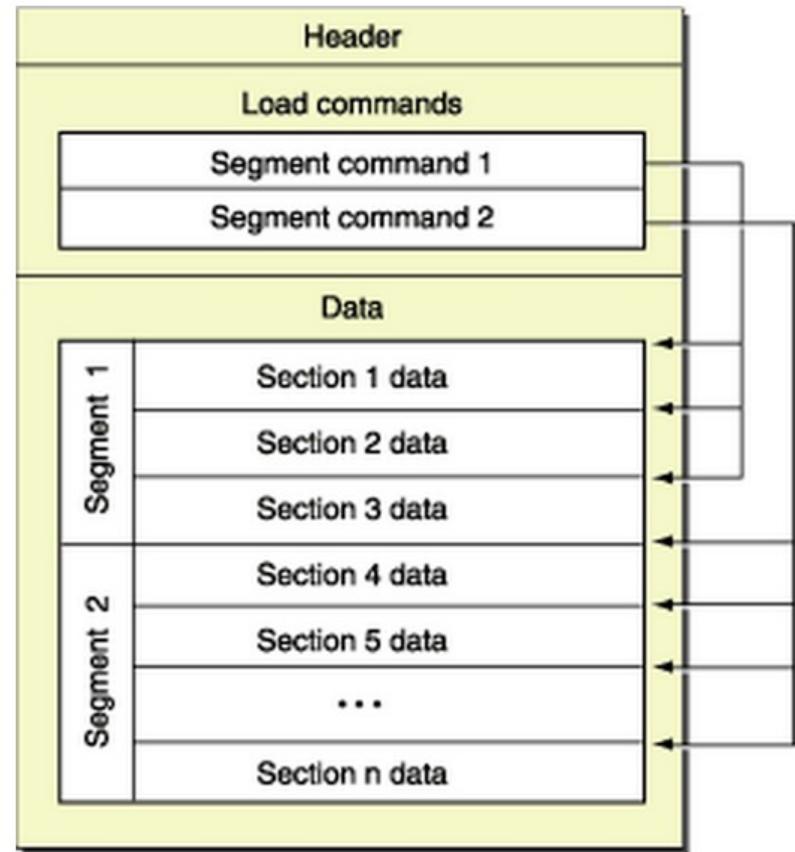
0x02 - O Formato Mach-O

Mach-O (Mach Object)

HEADER
LOAD COMMANDS
SECTIONS

Arquitetura do código objeto

ppc ppc64 i386 x86_64 armv6
armv7 armv7s arm64





0x02 - O Formato Mach-O

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 - O Formato Mach-O

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 - O Formato Mach-O

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 */
};

EXPORT_SYMBOL_GPL(mach_o_header);
EXPORT_SYMBOL_GPL(mach_o_header_size);
EXPORT_SYMBOL_GPL(mach_o_header_version);
```



0x03 – Tools - Análise (Estática / Dinâmica)

Análise Estática

- file
- strings
- editores hexa (**graphical**)
- lipo
- otool
- nm
- codesign
- machOView (**graphical**)
- hopper (**graphical**)
- class-dump

Análise Dinâmica

- xcode (**graphical**)
- ida Pro (**graphical**)
- llDb
- fseventer
- open snoop
- activity Monitor (**graphical**)
- procoxp
- tcpdump
- cocoaPacketAnalyzer (**graphical**)
- wireshark (**graphical**)
- lsock



0x03 – Tools - Análise (Estática)

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 - Análise (Estática)

STRINGS

```
logan /opt/malware/mach-o $ strings sample
IODeviceTree
text/html; charset=utf-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 - Análise (Estática) EDITORES HEXA

The screenshot shows three hex editor windows side-by-side:

- 0xED**: Top left, showing a file named "sample - Data".
- HexEdit**: Top right, showing a file named "wxHexEditor 0.23 Beta for Mac".
- wxHexEditor**: Bottom, active window, showing a file named "sample". It displays memory starting at address 00000000. The first four bytes (00000000, 00000001, 00000002, 00000003) are CA FE BA BE, which is highlighted with a yellow selection bar.

The wxHexEditor interface includes:

- Toolbar with Save, Copy, Cut, Paste, Undo, Redo buttons.
- Mode selector: Binary (radioed), 8 bit, 16 bit, 32 bit, 64 bit, Float, Double.
- Text search fields: "Text search" and "Find (Text search)".
- Offset and Value columns.
- Bottom status bar: Hex, Little Endian, Insert, ASCII, Offset: 0, Selection: 4.

0xED

HexEdit

wxHexEditor



0x03 – Tools - Análise (Estática)

LIPO

0xcafebabe

```
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 $
```



0x03 – Tools - Análise (Estática)

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 - Análise (Estática)

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 - Análise (Estática)

NM

```
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_$_NSMutableOrderedSet
    U __OBJC_CLASS_$_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
```



0x03 – Tools - Análise (Estática)

CODESIGN

```
1. Infected (bash)
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 - Análise (Estática)

MACH O VIEW

MachOView File Edit Format View Window Help

sample_01

RAW RVA

Search

Offset Data Description Value

Offset	Data	Description	Value
00000000	BEBAFECA	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,__progra...)
- ▶ Section64 (__DATA,__mod_i...)
- ▶ Section64 (__DATA,__nl_sy...)
- ▶ Section64 (__DATA,__la_sy...)
- Section64 (__DATA,__data)
- ▶ Dynamic Loader Info
- ▶ Symbol Table
- ▶ Dynamic Symbol Table
- String Table

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

Executable (PPC)



0x03 – Tools - Análise (Estática)

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
0000174c dyld_stub_binding_helper:
00001751 call 0x1751
00001752 pop eax
00001753 push dword [ds:eax+0x8bf]
00001758 mov eax, dword [ds:eax+0x8c3]
0000175e jmp eax
00001760 __dyld_func_lookup:
00001765 call 0x1765
00001766 pop eax
00001766 mov eax, dword [ds:eax+0xb3]
0000176c jmp eax

===== BEGINNING OF PROCEDURE

0000176e __init_daemon:
0000176f push ebp
00001770 mov ebp, esp
00001771 push ebx
00001772 sub esp, 0x14
00001773 call imp__jump_table_fork
00001775 test eax, eax
0000177a jne 0x178e

0000177e call imp__jump_table_setsid
00001783 xor ebx, ebx
00001785 call imp__jump_table_fork
0000178a test eax, eax
0000178c je 0x179a

> analysis section __dyld
> analysis section __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 - Análise (Estática)

CLASS-DUMP

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

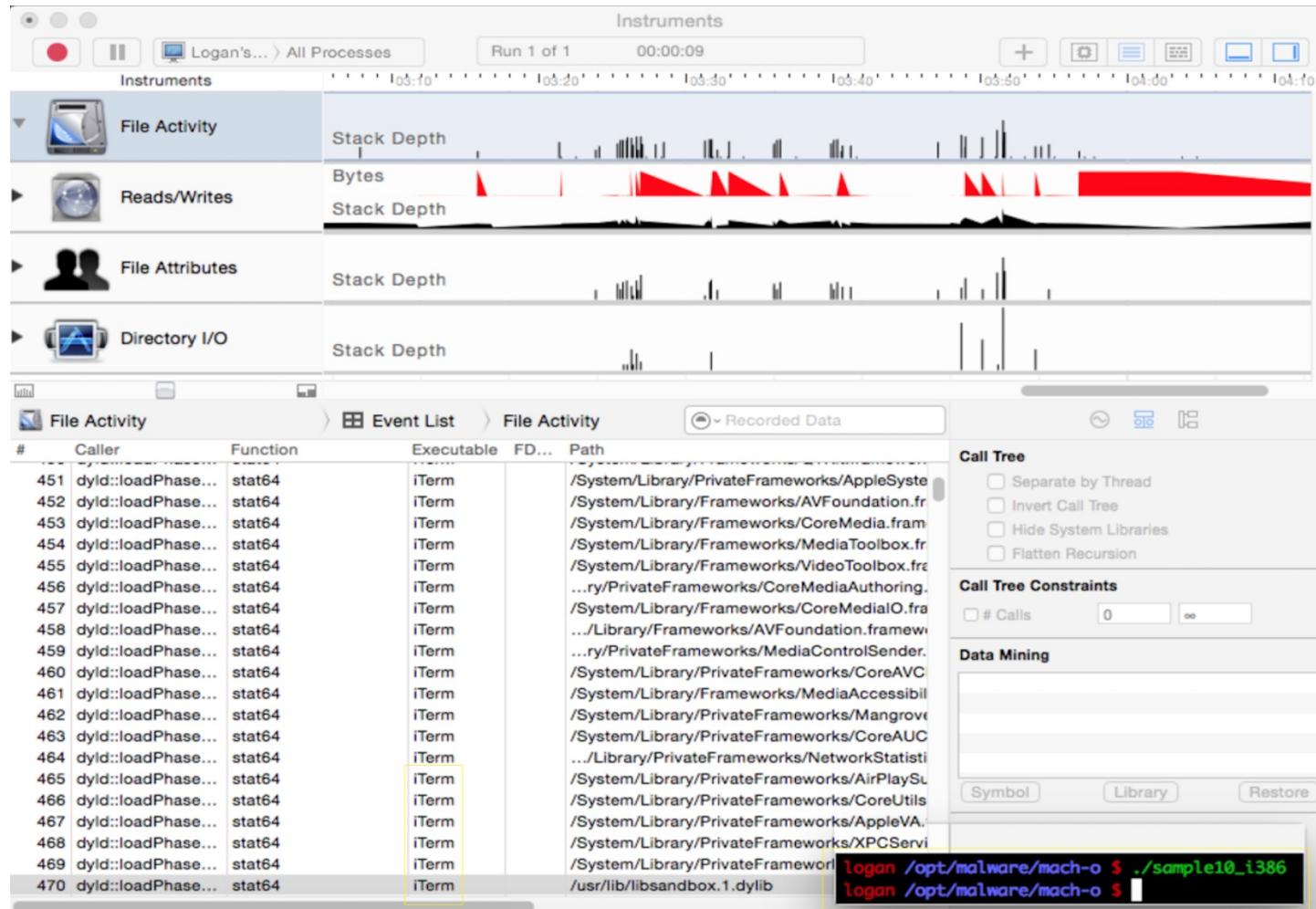
VMWARE FUSION / PARALLELS / VIRTUALBOX

- Manter o Software de Virtualização Atualizado
- Ferramentas de Sistema (Tools) Instaladas na VM
- Rede em modo Host-Only
- Se utilizar Pasta Compartilhada (Host) deixá-la como "somente leitura".
- Desativar o Gatekeeper (*Allow apps downloaded from: Anywhere*)



0x03 – Tools - Análise (Dinâmica)

XCODE





0x03 – Tools - Análise (Dinâmica)

IDA PRO

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

- File menu:** File, Edit, Jump, Search, View, Debugger, Options, Windows, Help.
- Toolbar:** Includes icons for file operations, search, and analysis.
- Functions window:** Lists functions: `__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:** Assembly view showing the following code:

```
; 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 shortlocret_1982
```
- Hex View A:** Hex dump view.
- Structures, Enums, Imports, Exports windows:** Standard IDA windows for defining data structures and imports/exports.
- Graph overview:** Shows a control flow graph with nodes and edges.
- Output window:** Displays logs and messages, including the compilation of idc files and the execution of the main function.
- Python window:** Shows the Python version and IDAPython license information.



0x03 – Tools - Análise (Dinâmica)

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[0xacc2] <+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[0xace2] <+54>: str r0, [sp, #0x1c]  
sample[0xace4] <+56>: movw r0, #0x14ec  
sample[0xace8] <+60>: movt r0, #0x0  
sample[0xacec] <+64>: movw r2, #0x1562  
sample[0xacf0] <+68>: movt r2, #0x0  
sample[0xacf4] <+72>: add r0, pc  
sample[0xacf6] <+74>: add r2, pc  
sample[0xacf8] <+76>: ldr r1, [r0]  
sample[0xacfa] <+78>: ldr r0, [r2]  
sample[0xacfc] <+80>: mov r5, r2  
sample[0xacfe] <+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 - Análise (Dinâmica)

FSEVENTER

The screenshot shows the FSEVENTER application interface. At the top, there's a menu bar with Apple, fseventer, File, Edit, Window, Help. To the right of the menu is a status bar showing a monitor icon, "Wed 5:10 PM", a search icon, and a list icon. Below the menu is a toolbar with icons for file operations. The main area is a file browser titled "fseventer - Stopped". It displays a hierarchical file structure with various files and folders. A yellow selection box highlights a path: "/private/tmp/CurlUpload/2A303B77-ABE2'35 minutes old'762B26E04E5sample_03". Inside this box, several files are listed: "Chown", ".con'back", "LaunchAgents", "checkvir.plist", "checkvir", "com.apple.spaces.plist", "com.apple.spaces.plist.t9kyHoV", "com.fernlightning.fseventer.plist", "com.fernlightning.fseventer.plist.BeYAcAv", "Saved Application State", "com.googlecode.iterm2.savedState", "windows.plist", "window_2.data", "window_1.data", "window_2.data", "windows.plist", and "data.data". To the right of the browser, there's a terminal window with the title "1. Infected (sample_03)". The terminal output is:
logan /opt/malware/mach-o \$./sample_03
user=logan
file name is :./sample_03
ret = 6 (write_error = 0)
[]

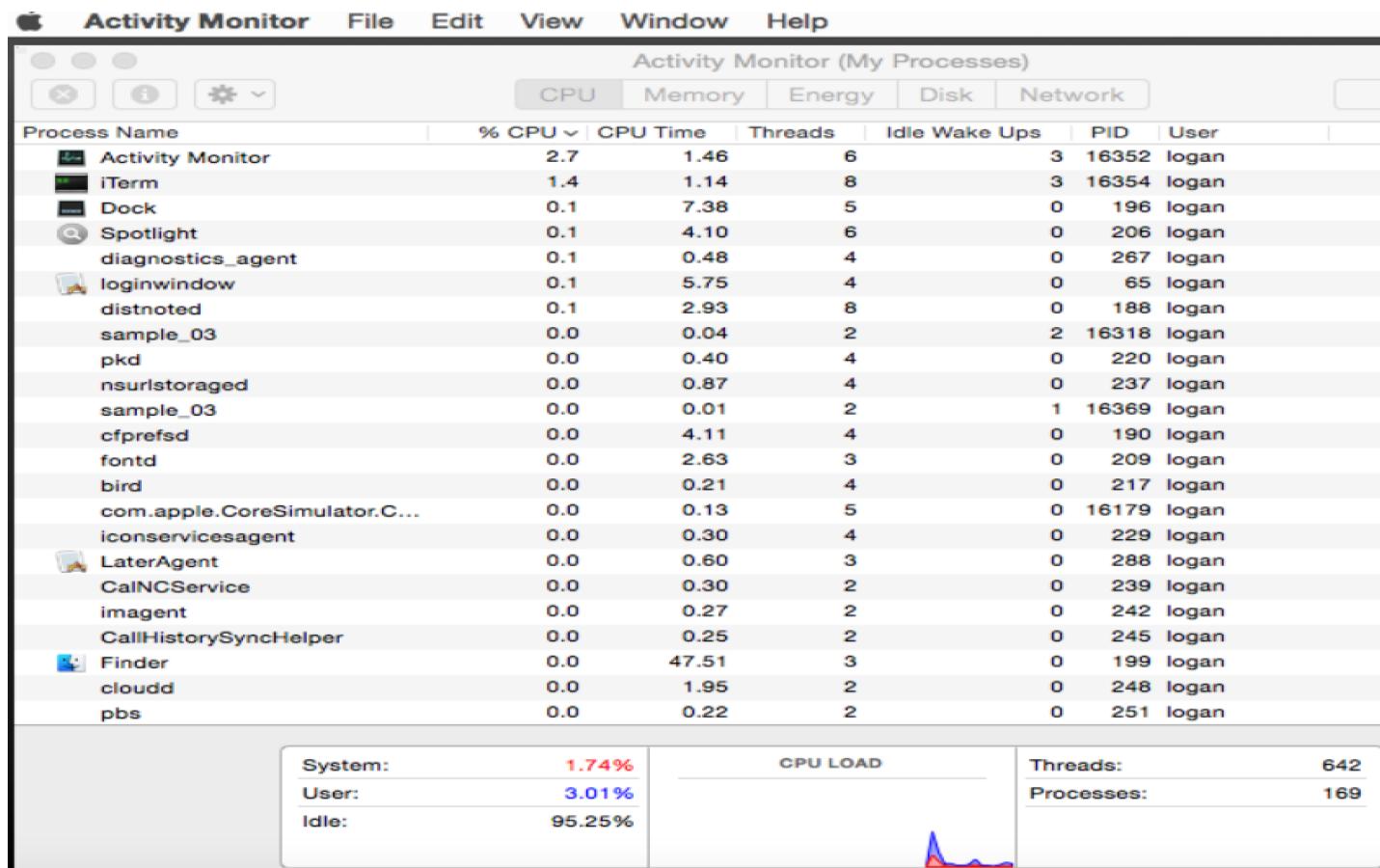


0x03 – Tools - Análise (Dinâmica) OPEN SNOOP

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.suvavetech.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 - Análise (Dinâmica) **ACTIVITY MONITOR**





0x03 – Tools - Análise (Dinâmica)

PROCXP

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 - Análise (Dinâmica)

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 - Análise (Dinâmica)

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 2E 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 - Análise (Dinâmica) WIRESHARK



WIRESHARK



0x03 – Tools - Análise (Dinâmica)

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



0x04 – Ameaças Atuais

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 – Ameaças Atuais



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)

1 1

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

Fonte: www.virustotal.com



0x04 – Ameaças Atuais



SHA256:	8faa03fb71638494edd93b02e327b0f48da7e1c6c8a0c724ea9c68e259d31480	
Nome do arquivo:	stty5_1.11.pl	
Taxa de detecção:	34 / 57	
Data da análise:	2015-04-20 02:45:18 UTC (1 dia, 11 horas atrás)	
Antivírus	Resultado	Atualização
ALYac	MAC.IOS.WireLurker.B	20150420
AVG	OSX/WireLurker.A	20150420
AVware	Trojan.OSX.Wirelurker.co (v)	20150420
Ad-Aware	MAC.IOS.WireLurker.B	20150420
Avast	MacOS:WireLurker-F [Trj]	20150419
Avira	MACOS/WireLurker.A.5	20150419
BitDefender	MAC.IOS.WireLurker.B	20150420
CAT-QuickHeal	Trojan.IOS.WireLurker.D	20150418
ClamAV	OSX.Trojan.Wirelurker-1	20150420
Comodo	UnclassifiedMalware	20150419
Cyren	MacOS/WireLurker.A	20150420

Fonte: www.virustotal.com



0x04 – Ameaças Atuais

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

Fonte:

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

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



0x04 – Ameaças Atuais

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)

binário:

/tmp/.z

Fonte:

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/osx_kaiten.a



0x04 – Ameaças Atuais

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)

Fonte:

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/osx_careto.a



0x05 – Conclusão

Hacking is a way of life

Referência:

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

Obrigado!
Perguntas ?

Contato

ricardologanbr@gmail.com
@l0ganbr