O MAIOR EVENTO DE HACKING, SEGURANÇA E TECNOLOGIA ~~DO BRASIL~~ DO CONTINENTE

ROADSEC

MACH-O

A NEW THREAT

$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.

Member # RTFM 💀 Co|\|cL/\V€ #

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 / Q & (MAYBE \0/) A

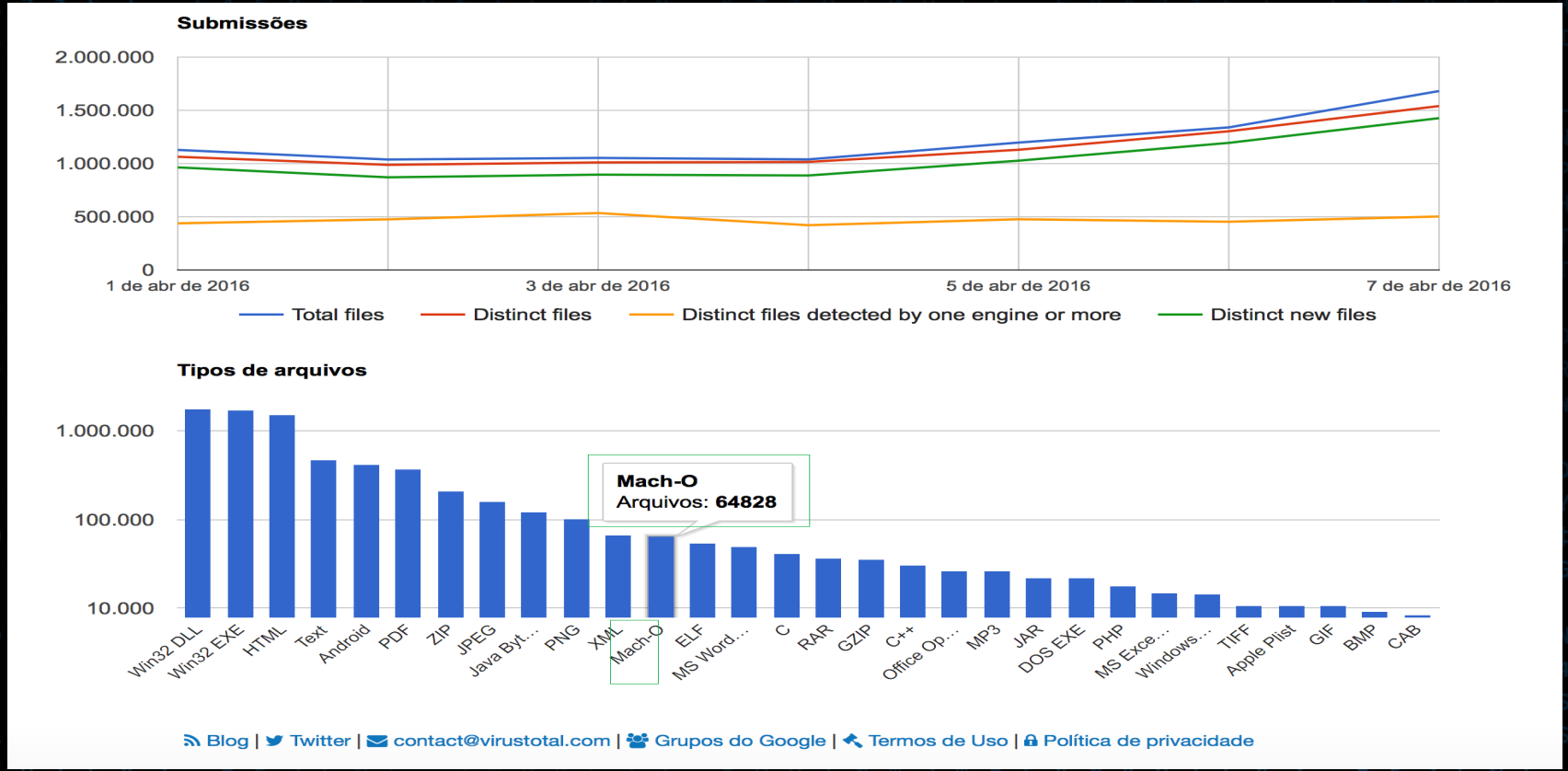
0x00 - Motivation of Research

Windows always gets infected!!!

Does Linux ever gets infected??

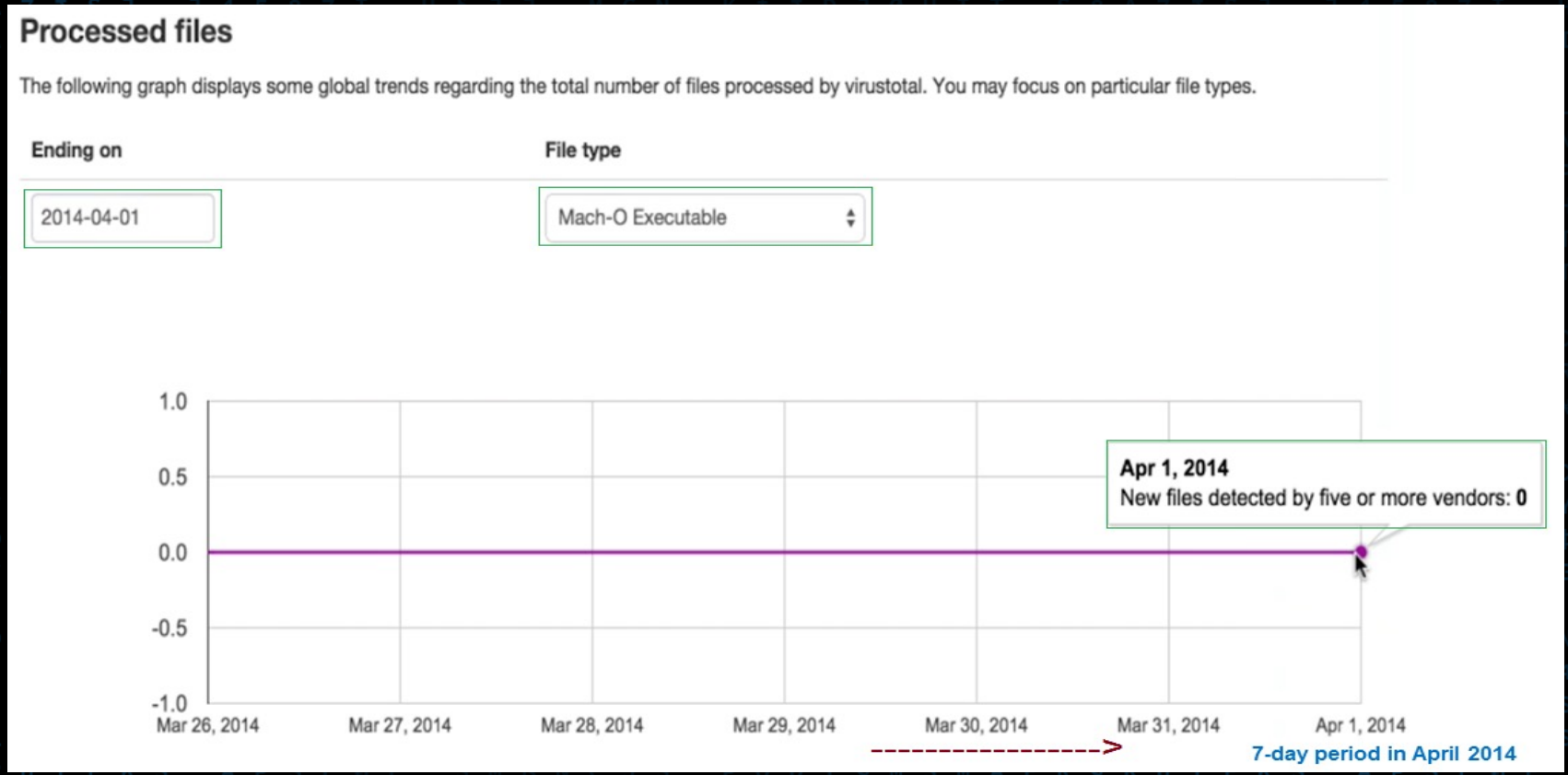
“Mac OS ever gets infected…”

0x01 - OS X, The New Target



Source: www.virustotal.com

0x01 - OS X, The New Target



Source: www.virustotal.com

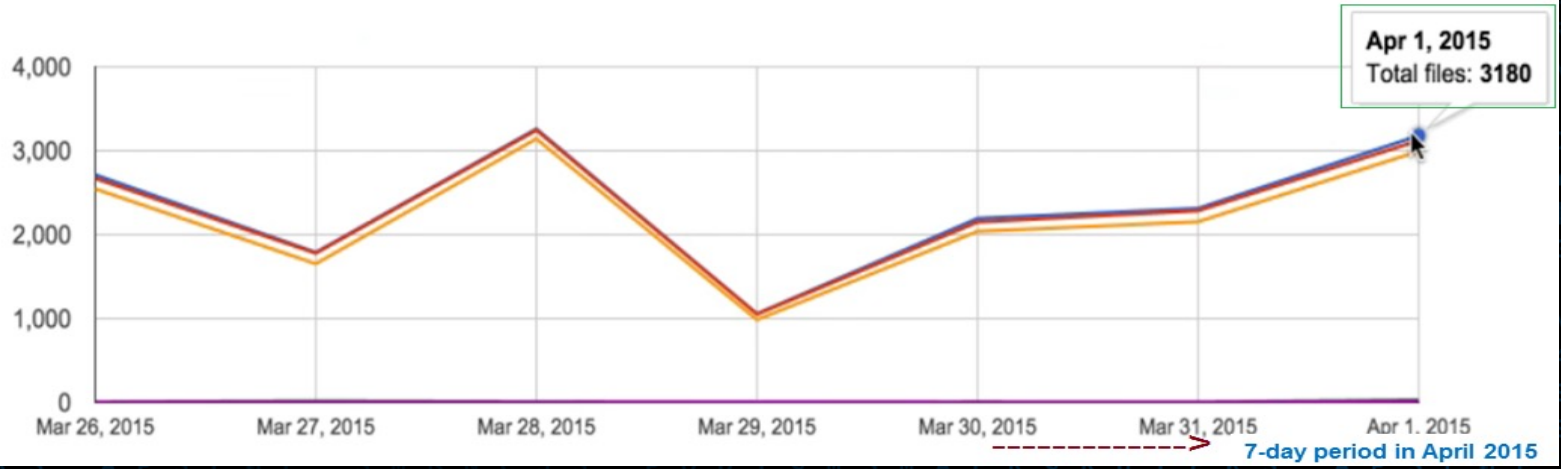
0x01 - OS X, The New Target

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.

Ending on 2015-04-01

File type Mach-O Executable



Source: www.virustotal.com

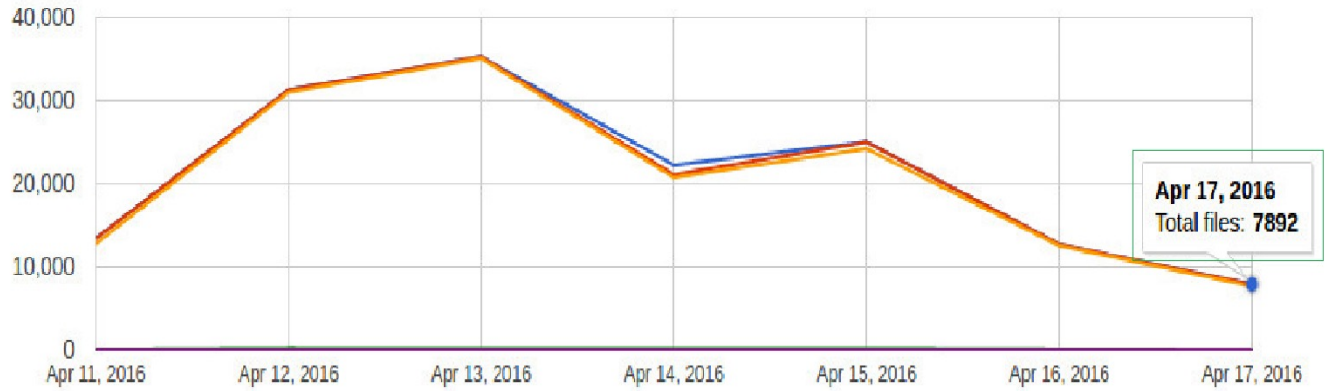
0x01 - OS X, The New Target

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.

Ending on: 2016-04-17

File type: Mach-O Executable



----------> Period (April 2016)

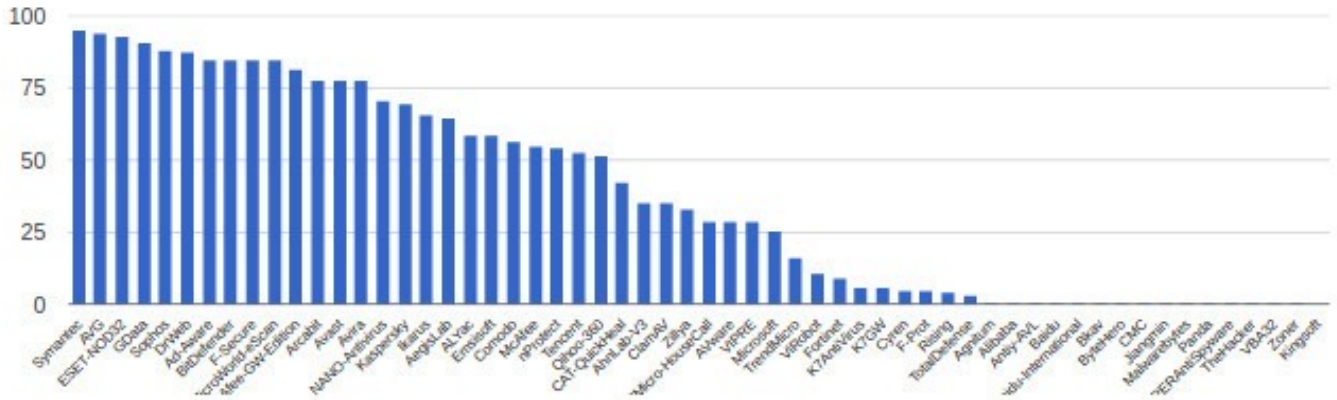
Source: www.virustotal.com

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?

Submitted on	Age	Positives	Type
2016-03-24	Any	5+	Mach-O Executable



Source: www.virustotal.com

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 were 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)

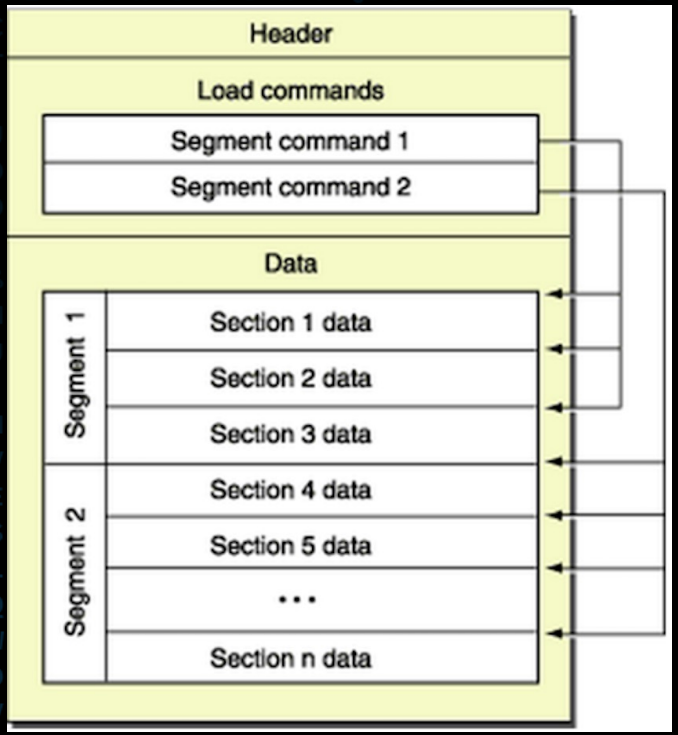
0x02 - The Mach-O Format

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

ROADSEC

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

ROADSEC

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

ROADSEC

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 (Static / Dynamic)

Análise Estática

- file
- strings
- upx
- 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
- wireshark (graphical)
- lsock
- little Snitch (graphical)

0x03 – Tools (Static)

```
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 $
```

FILE

mach-o

0x03 – Tools (Static)

STRINGS

```
logan /opt/malware/mach-o $ strings sample
IODeviceTree
text/html; charset=utf-8
;/?:@&=+$
%@=%@&
POST
application/x-www-form-urlencoded; charset=utf-8
Content-Type
text/html
Accept
no-cache
Cache-Control
Pragma
close
Connection
something is wrong: %@
CFBundleExecutable
http://www.comeinbaby.com/start_log/?app=%@&sn=%@
serial-number
kill -HUP SpringBoard
mv "%@" "%@"
_objc_autoreleasePoolPush
_objc_autoreleasePoolPop
__TEXT
__LINKEDIT
_object_setInstanceVariable
_object_setIvar
_object_copy
_objc_retain
_objc_retainBlock
_objc_release
```

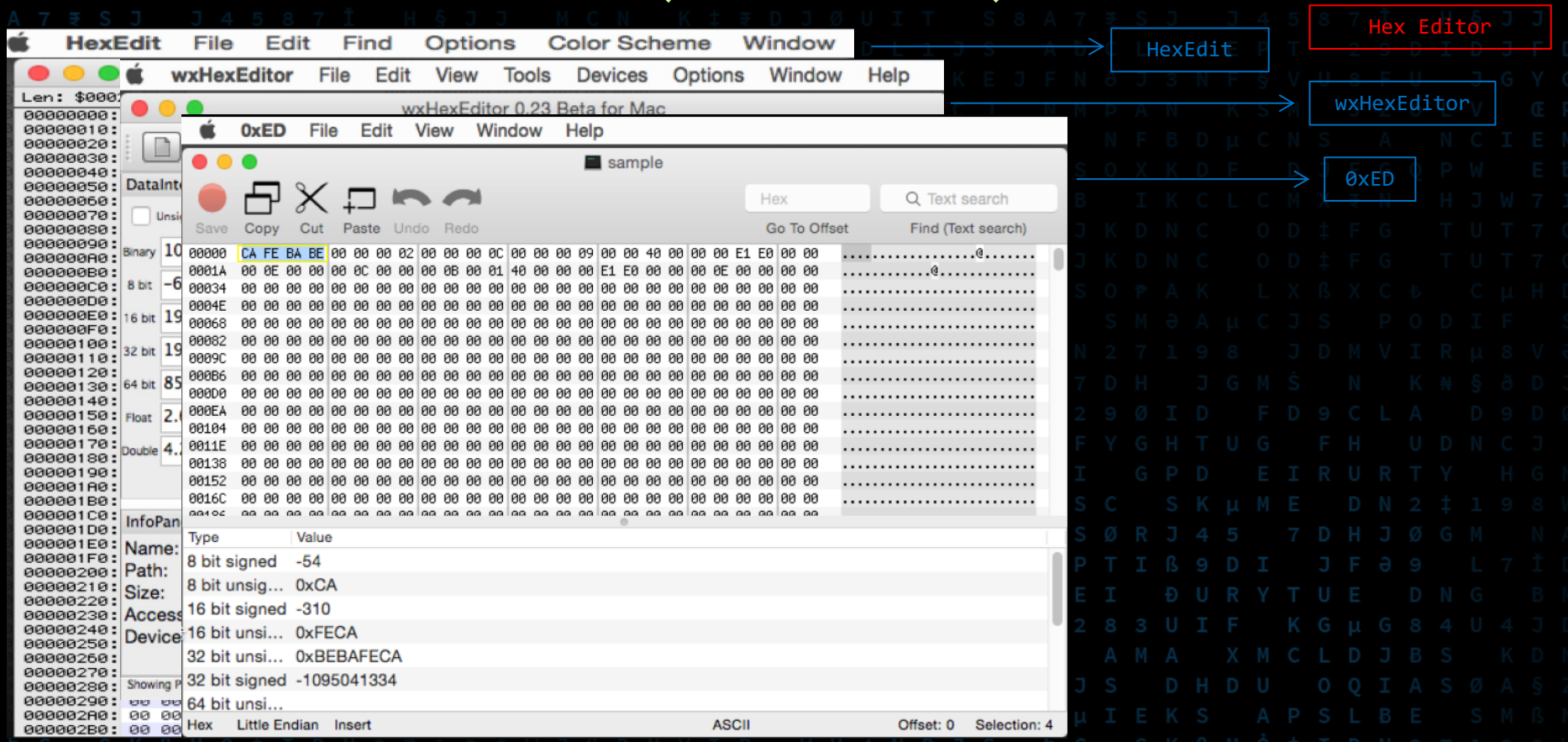
0x03 – Tools (Static)

BINWALK / UPX

```
logan /opt/malware/mach-o $ upx -t *
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.09        Markus Oberhumer, Laszlo Molnar & John Reiser   Feb 18th 2013

upx: headers_samples01: IOException: not a regular file -- skipped
upx: malware: IOException: not a regular file -- skipped
upx: malware.zip: NotPackedException: not packed by UPX
upx: old: IOException: not a regular file -- skipped
testing sample [OK]
upx: sample10_i386: NotPackedException: not packed by UPX
upx: sample_01: NotPackedException: not packed by UPX
testing sample_02 [OK]
testing sample_03 [OK]
upx: sample_04: NotPackedException: not
upx: sample_05: NotPackedException: not
upx: sample_06: NotPackedException: not
upx: sample_07: NotPackedException: not
upx: sample_08: NotPackedException: not
upx: sample_09: NotPackedException: not
upx: sample_10: NotPackedException: not

Tested 3 files.
```

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

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
9087          0x237F          Copyright string: "Copyright (C) 1996-2013 the UPX Team. All Rights
 Reserved. $"

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

0x03 – Tools (Static)



0x03 – Tools (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 $
```

0xcafebabe

LIPO

0x03 – Tools (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 (Static)

```
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)
```

OTOOL

0x03 – Tools (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 _IORegistryEntrySearchCFProperty
         U _IORegistryGetRootEntry
         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__
```

NM

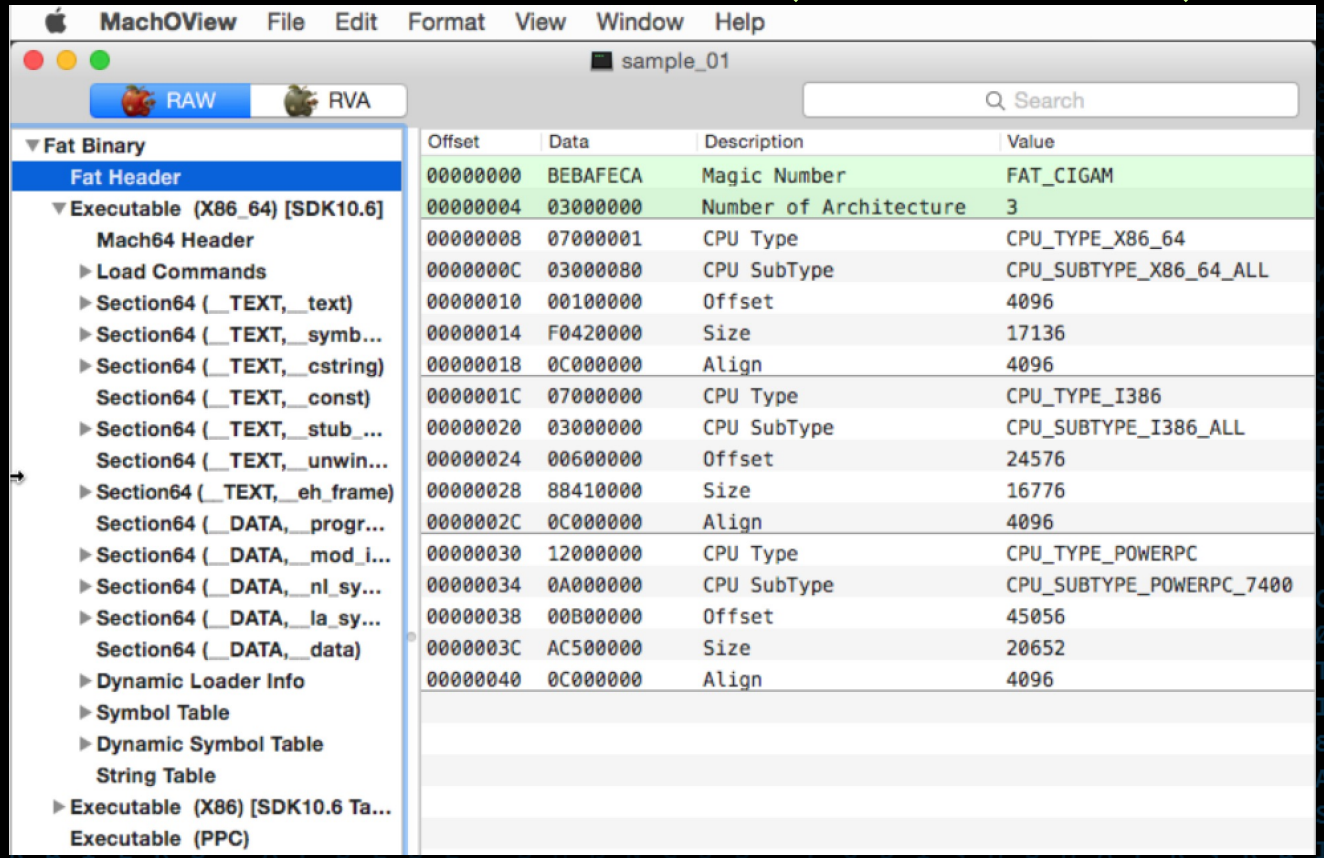
0x03 – Tools (Static)

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 (Static)

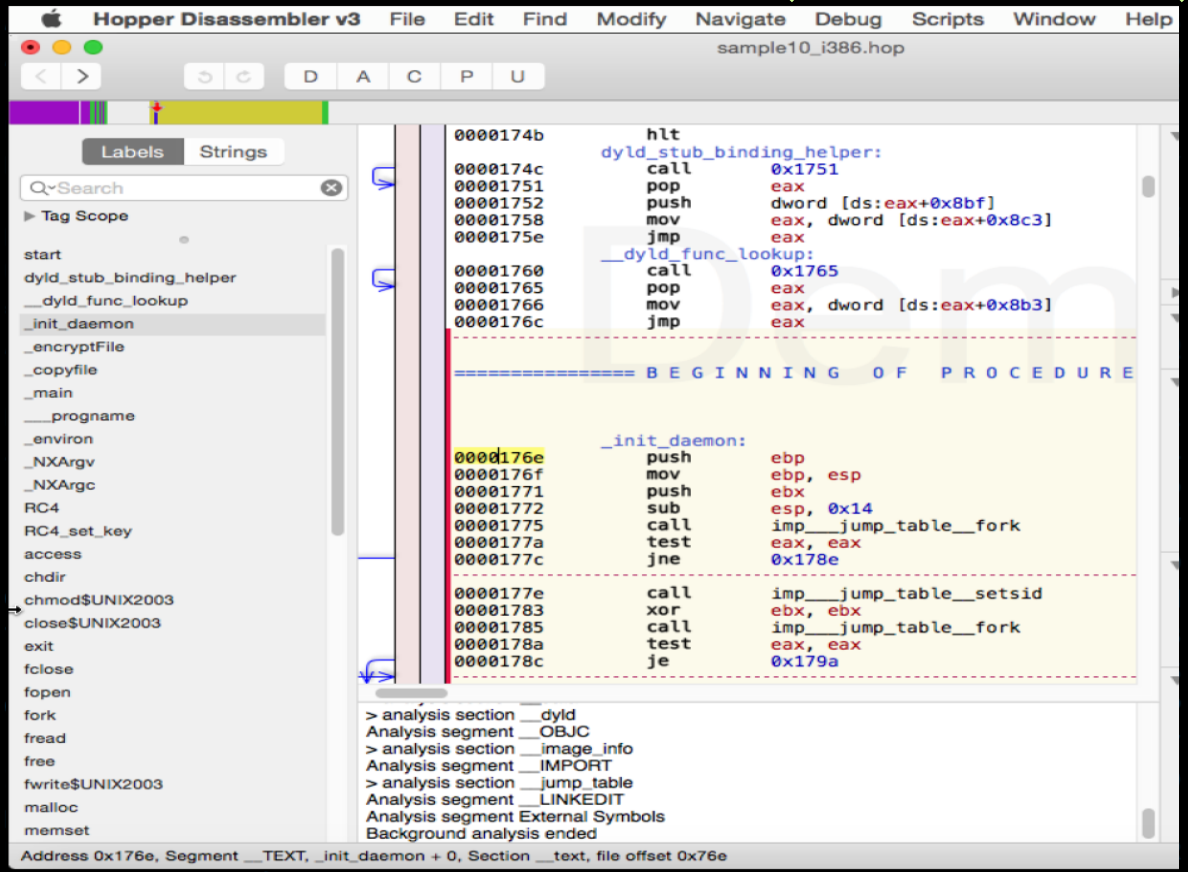
MachOView



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

0x03 – Tools (Static)

HOPPER



0x03 – Tools (Static)

CLASS-DUMP

```
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 $
```

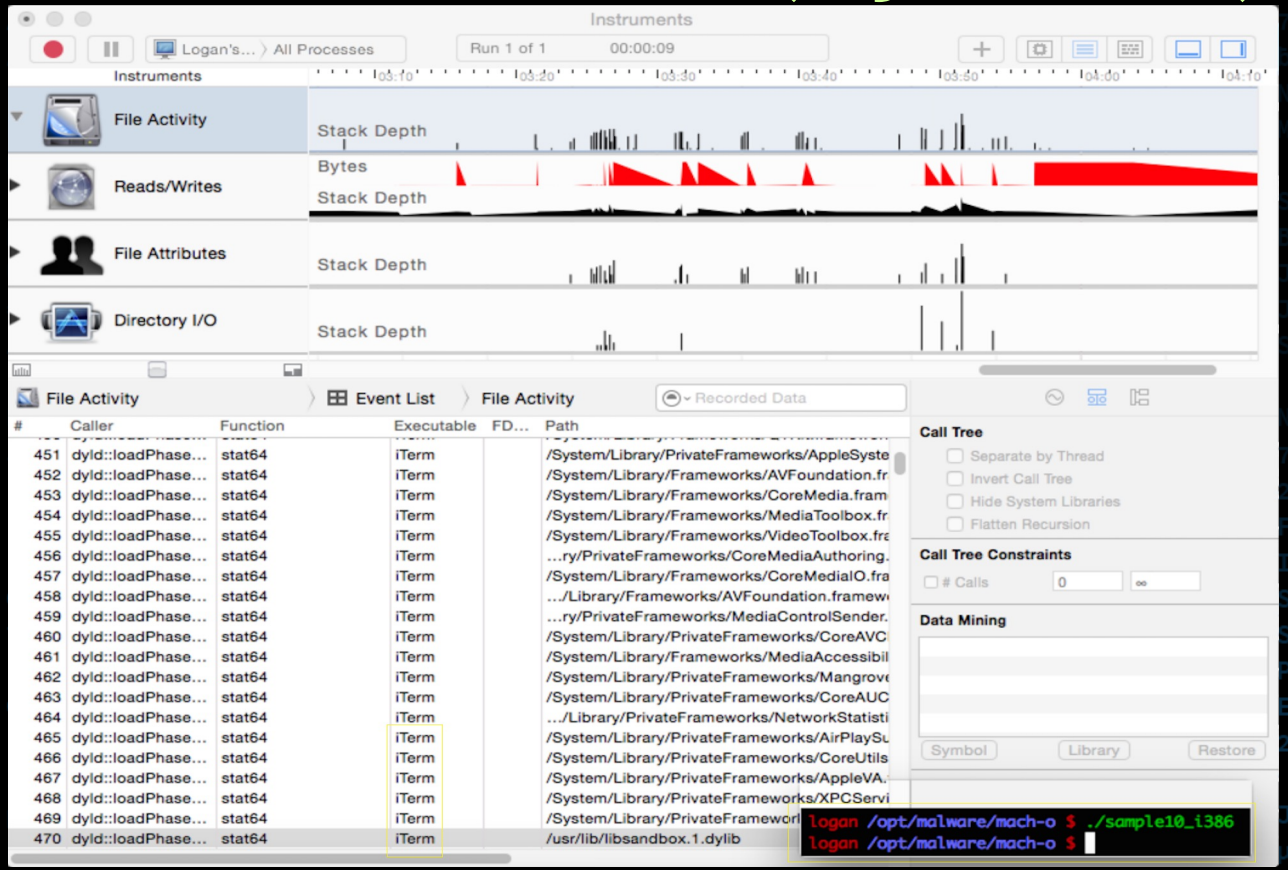
0x03 – Tools (Dynamic)

VMWARE FUSION / PARALLELS / VIRTUALBOX

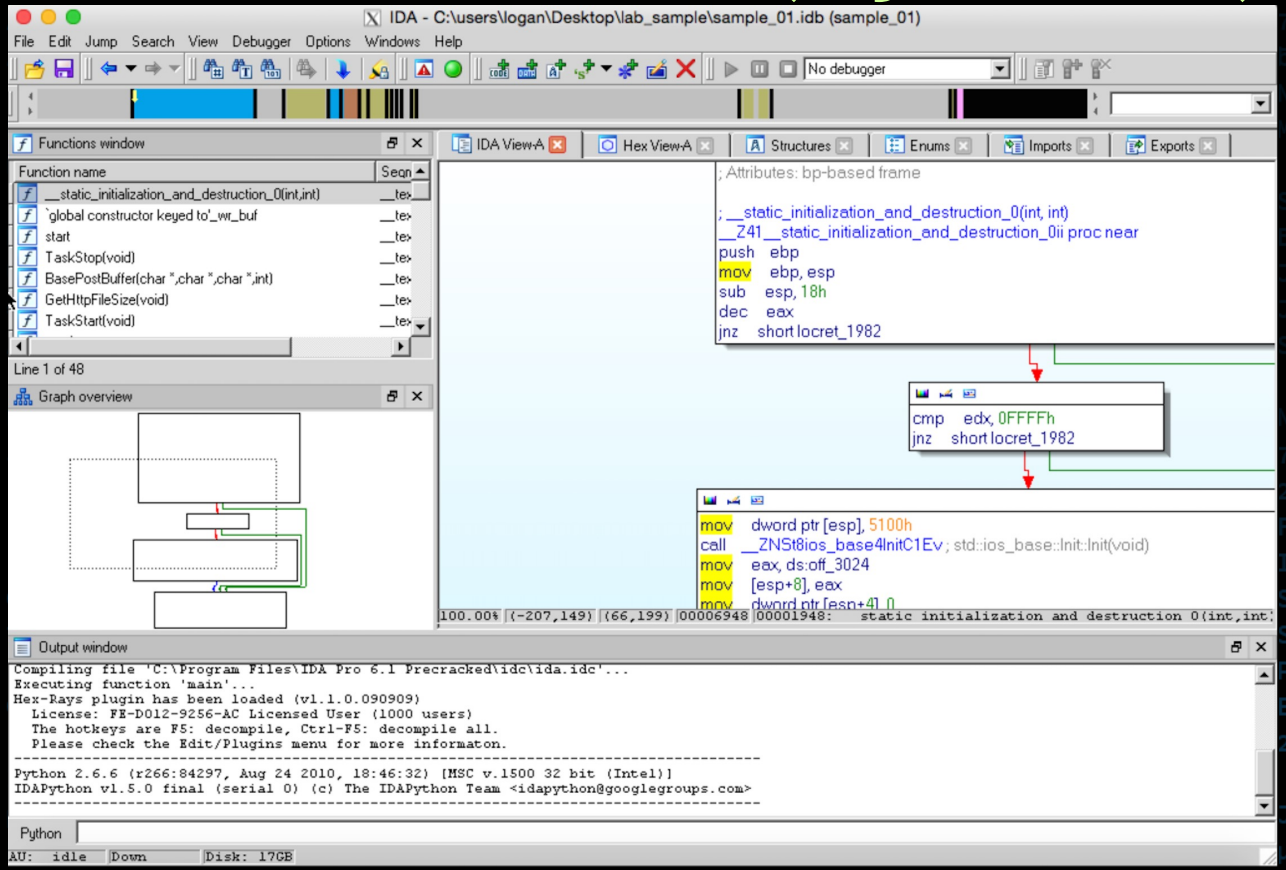
- Keep Virtualization Software Updated
- Use System Tools Installed in VM
- Network Host-Only mode
- If you use Shared Folder(Host) leave it as “read-only”
- Disable Gatekeeper (Allow apps downloaded from: Anywhere)

0x03 – Tools (Dynamic)

XCODE



0x03 – Tools (Dynamic)



IDA PRO

Also is Static Tool

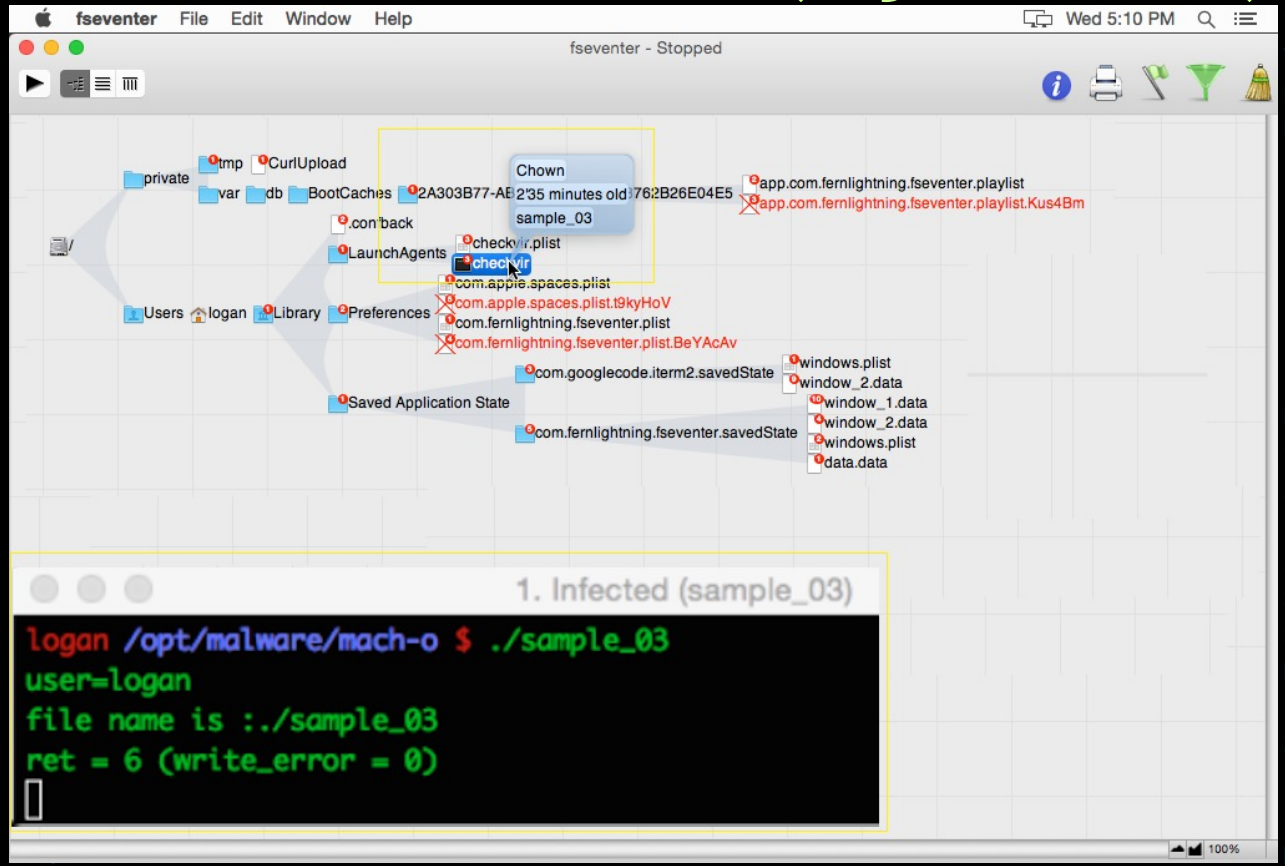
0x03 – Tools (Dynamic)

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[0xacc2] <+22>:  movt   r2, #0x0
sample[0xacc6] <+26>:  add    r0, pc
sample[0xacc8] <+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[0xacd6] <+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]
```

0x03 – Tools (Dynamic)

FSEVENTER



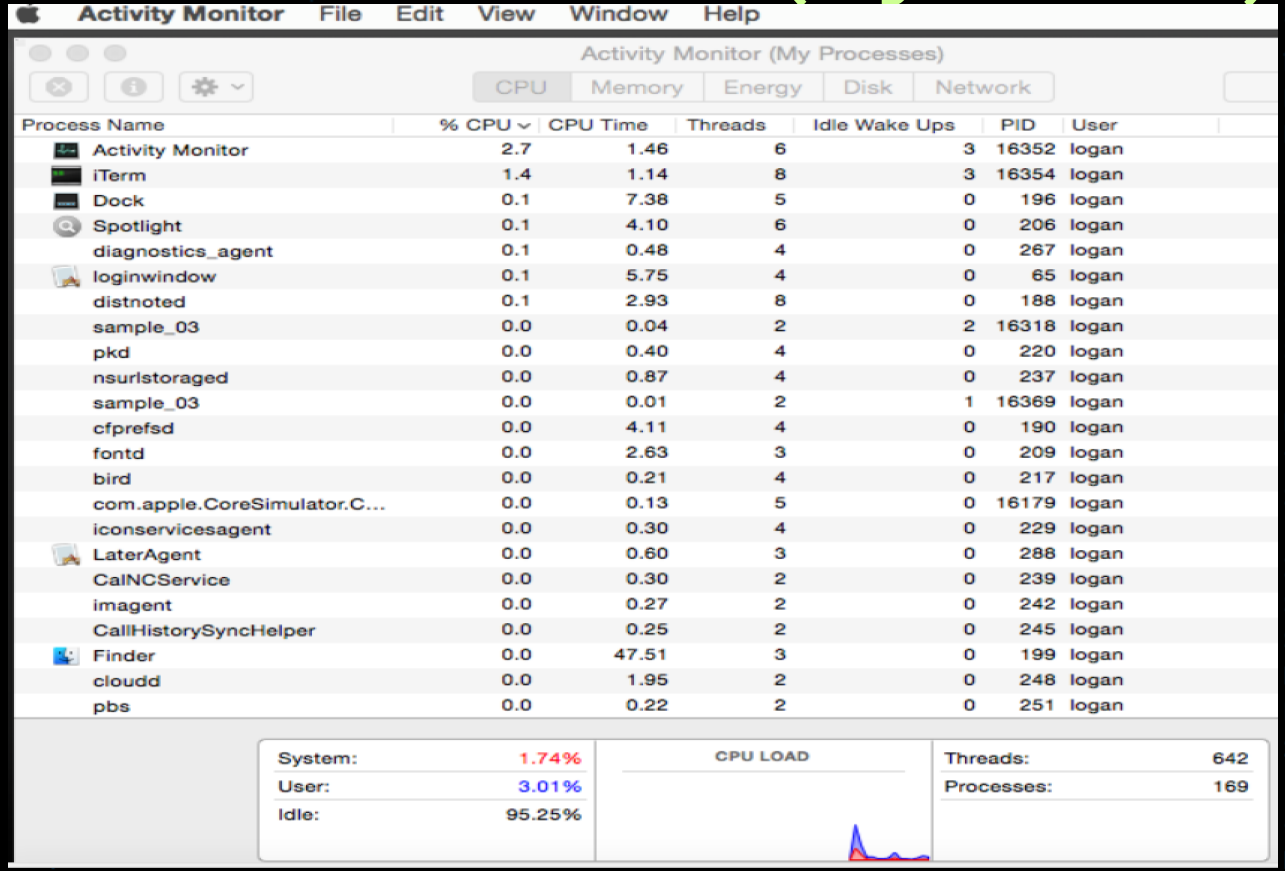
0x03 – Tools (Dynamic)

OPEN SNOOP

```
logan ~ $ sudo opensnoop -a
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/69650876-3F59-9236-5
5DF-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 c
fprefsd\0
1684624901     2015 Apr 22 04:23:12   501    190   4   0 /Users/logan/Library/Preferences/ByHost/com.apple.loginwindow.564
D4EC2-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.s
uavetech.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.Launc
hServices-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
```

0x03 – Tools (Dynamic)

ACTIVITY MONITOR



0x03 – Tools (Dynamic)

PROCXP

```
04:59:35  Up 06:03:40 Load Average:  1.19 1.03 0.83
CPU:   3/3 active <Unable to get processor information>
RAM:  1699M Free + 1370M Used (Active:  764M + Inactive:  166M + Wired:  439M Comp:    0M)   36M purgeable
          Memstatus: 85 Comp:    0M + Decomp:    0M  File: 1585M  Anon:  596M Throttled:    0M
Pkts:  TX: 13513/1M (0 bytes/sec)  RX: 10785/838K (0 bytes/sec)
Unable to get Power Source information
```

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	2929M	10M	S	04:59:23	00.20	0	21	----	----
729	1	501	none	mdworker	4	3	2430M	7832K	S	04:59:21	00.04	0	5	----	----
726	1	501	none	syncdefaultsd	31	2	2422M	13M	S	04:59:08	00.12	0	4	----	----
725	296	501	268435	procexp.univers	31	4/1	2443M	45M	R	04:59:06	00.84	48	5	0B	0B
578	1	501	none	helpd	4	2	2422M	5416K							
456	1	501	none	USBAgent	31	2	2400M	5276K							
417	1	501	none	nbagent	4	4	2467M	13M							
365	1	501	none	mdflagwriter	31	2	2400M	812K							
345	1	501	none	EscrowSecurityA	4	3	2466M	15M							
313	1	501	none	storedownloadd	4	2	2424M	7492K							
312	1	501	none	LaterAgent	31	3	2466M	11M							
311	1	501	none	storeassetd	4	2	2428M	8924K							
310	1	501	none	storelegacy	4	2	2400M	6220K							
296	295	501	268435	bash	31	1	2394M	1324K							
292	1	501	none	CoreServicesUIA	31	3	2478M	12M							
285	1	501	none	com.apple.Input	4	2	2422M	7144K							
283	1	501	none	iTerm	31	7	2565M	62M							
281	1	501	none	AppleSpell	31	2	2424M	3048K							
280	1	501	none	pbs	4	2	2425M	3580K							
275	1	501	none	com.apple.notif	4	2	2400M	8996K							
273	1	501	none	com.apple.metad	4	5	2427M	12M							
272	1	501	none	CalNCService	4	2	2428M	17M							

```
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      0K  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)
```

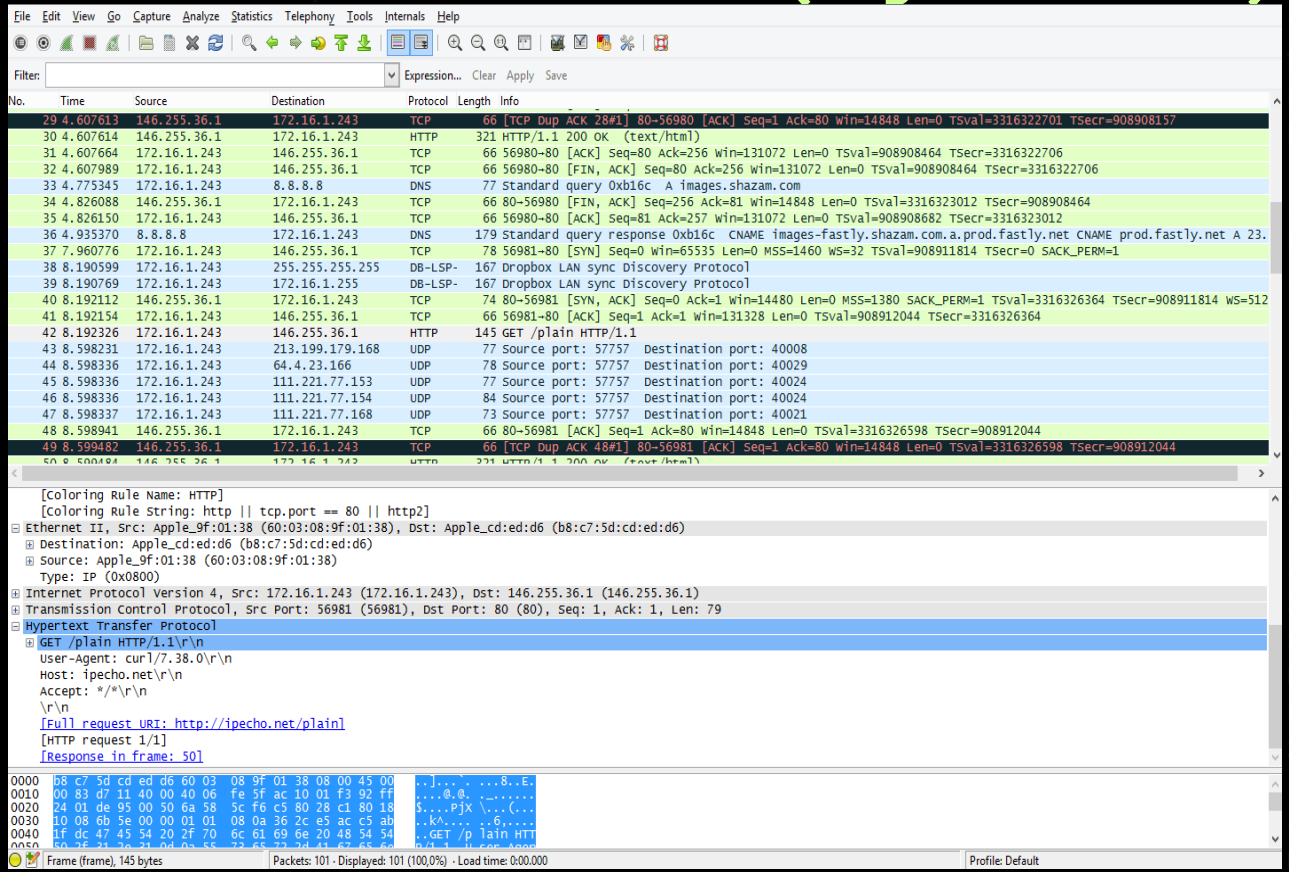
0x03 – Tools (Dynamic)

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 (Dynamic)

WIRESHARK



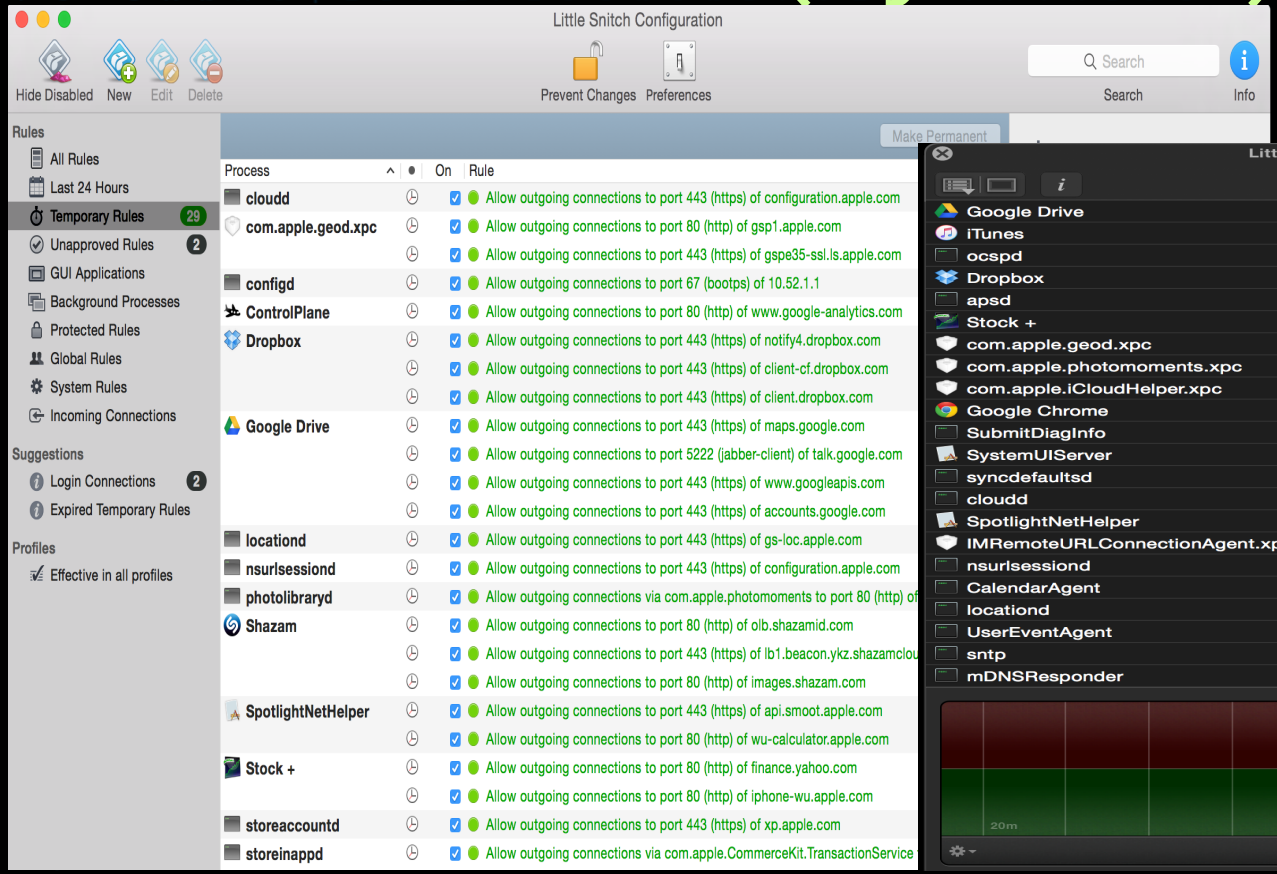
0x03 – Tools (Dynamic)

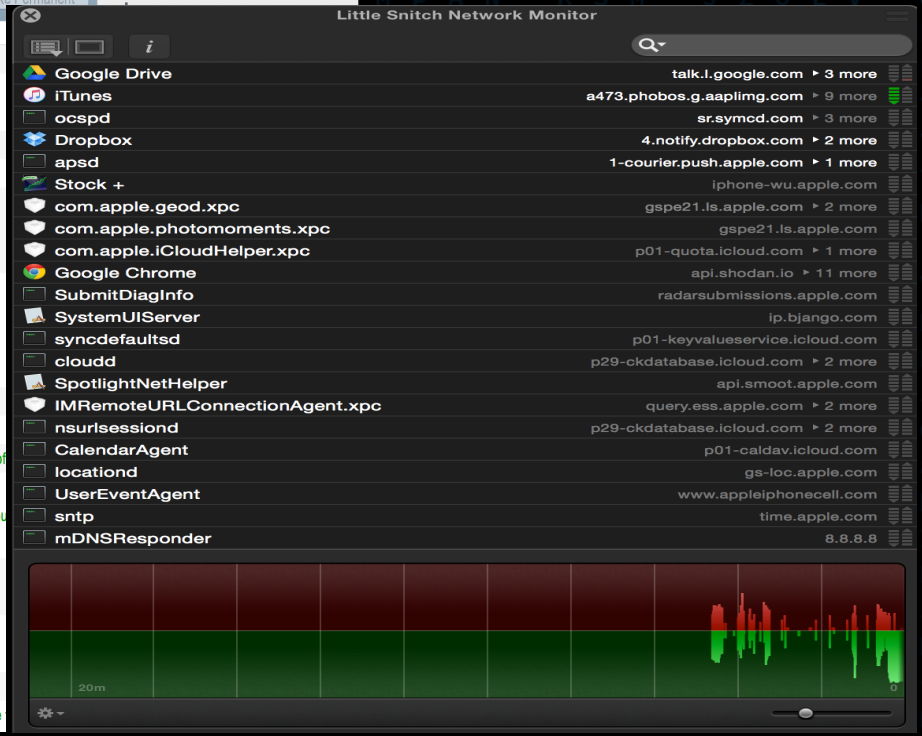
LSOCK

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 (Dynamic)

Little Snitch





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

OSX_KAITEN.A

Names: MacOS_X/Tsunami.A (Microsoft),
OSX/Tsunami (McAfee),
OSX/Tsunami-Gen (Sophos),
OSX/Tsunami.A (F-Secure),

Binary:
/tmp/.z

OSX_CARETO.A

Names: MacOS:Appetite-A [Trj] (Avast)
OSX/BackDoor.A (AVG)
Trojan.OSX.Melgato.a (Kaspersky)
OSX/Backdoor-BRE (McAfee)
Backdoor:MacOS_X/Appetite.A (Microsoft)
OSX/Appetite-A (Sophos)

itunes212.{BLOCKED}pdt.com

0x04 – Current Threats (MacOS:KeRanger-C)

On March 2016 appear the first Ransoware writing for mach-o file on OSX System (KeRanger), Distributed by client BitTorrent Transmission (v.2.90) This threat has been fixed in version v.2.91 the client.
The latest version Gatekeeper OSX already block this ransoware since the first sample published \0/!!!

```
logan@Infected /opt/malware/osx/Ransomware.OSX.KeRanger_samples  $ ll
total 13M
drwx------ 2 logan logan 4,0K Mar 11 22:53 .
drwxrwxr-x 3 logan logan 4,0K Mar 11 20:59 ..
-rw-r--r-- 1 logan logan 136K Dez  1  2107 14a4df1df622562b3bf5bc9a94e6a783 _General.rtf_
-rw-r----- 1 logan logan 5,0M Mar  5 15:03 1d6297e2427f1d00a5b355d6d50809cb _Transmission-2.90.dmg_d1ac55
-rw-r----- 1 logan logan 5,0M Mar  5 15:03 24a8f01cfdc4228b4fc9bb87fedf6eb7_Transmission-2.90.dmg_d7d765
-rw-r--r-- 1 logan logan 1,3M Dez  1  2107 3151d9a085d14508fa9f10d48afc7016 _Transmission
-rw-r--r-- 1 logan logan 1,3M Dez  1  2107 56b1d956112b0b7bd3e44f20cf1f2c19 _Transmission
-rw-r--r-- 1 logan logan 136K Dez  1  2107 861c3da2bbce6c09eda2709c8994f34c _General.rtf_
logan@Infected /opt/malware/osx/Ransomware.OSX.KeRanger_samples  $ file *
14a4df1df622562b3bf5bc9a94e6a783 _General.rtf_:                Mach-O 64-bit executable
1d6297e2427f1d00a5b355d6d50809cb _Transmission-2.90.dmg_d1ac55: bzip2 compressed data, block size = 100k
24a8f01cfdc4228b4fc9bb87fedf6eb7_Transmission-2.90.dmg_d7d765:  bzip2 compressed data, block size = 100k
3151d9a085d14508fa9f10d48afc7016 _Transmission:                Mach-O 64-bit executable
56b1d956112b0b7bd3e44f20cf1f2c19 _Transmission:                Mach-O 64-bit executable
861c3da2bbce6c09eda2709c8994f34c _General.rtf_:                Mach-O 64-bit executable
```

0x04 – Current Threats (MacOS:KeRanger-C)

```
logan@Infected /opt/malware/osx/KeRanger  $ cat info2.txt

14a4df1df622562b3bf5bc9a94e6a783\

lclebb6kvohlkcml.onion.link
lclebb6kvohlkcml.onion.nu
bmacyzmea723xyaz.onion.link
bmacyzmea723xyaz.onion.nu
nejdtkok7oz5kjoc.onion.link
nejdtkok7oz5kjoc.onion.nu

Owner ou Group: POLISAN BOYA SANAYI VE TICARET ANONIM SIRKETI1

osx/ping?user_id=%s&uuid=%s&model=%s
```

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

Thanks for my wife and brothers (C00ler,Clandestine, Slayer, Unknow_Antisec, DMR, BSDaemon, Robertux, RTFM Team and OSX_Rev)

Thanks a Lot
Any Questions ?

ROADSEC

#dontstophacking

Contact: ricardologanbr@gmail.com
@l0ganbr