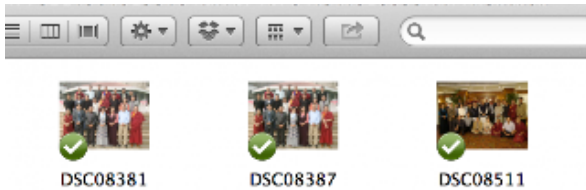


Group Photos.zip OSX/Revir | OSX/iMuler samples March 2012- November 2012

Archived: 2026-04-05 20:30:56 UTC

[Group Photos.zip OSX/Revir | OSX/iMuler samples March 2012-November 2012](#)



Sophos posted information about a variant of iMuler OSX trojan targeting Tibet activists ([New variant of Mac Trojan discovered, targeting Tibet](#)) and posted the MD5 2d84bfbae1f1b7ab0fc1ca9dd372d35e (FileAgent 37.3 KB) of the trojan . This post is for the actual dropper, which is a full 1.9 MB package (Group photo.zip MD5: 9e34256ded3a2ead43f7a51b9f197937)

I don't have a Mac OS VM handy tonight to provide more details about the traffic or behavior so I will just describe the package and post the previous version of the same trojan that was targeting fans of Russian topless models.

Download



October 2012

File: Group photo.zip Size: 1976395

MD5: 9E34256DED3A2EAD43F7A51B9F197937

1. 7dba3a178662e7ff904d12f260f0fff3 (Installer)
2. 9d2462920fdaed5e360875fb0cf8274f (malicious payload)
3. D029E0D44F07F9F4566B0FCE93D8A17E (payload variant)
4. e00a280ad29440dcaab42ad093bcaafd (uploader module)

File Information

Just like [the previous version of iMuler](#), this trojan hides inside a zip package with application bundle files .app disguised as photos. Default installation of Mac OS will show those app files like any images files - see above. Clicking on them to expand would install the trojan.

The screenshot made from Windows and list of files shows clearly that these are not just images.



|——DSC08381.app

| |——Contents

| | | Info.plist

| | | PkgInfo

| | |

| |——MacOS

| | | .cnf

| | | **.confr <<<< Image file**

| | | .conft



| | FileAgent <<<< MD5: 2D84BFBAE1F1B7AB0FC1CA9DD372D35E

[\(VirusTotal 6/44\)](#)

| |

| |——Resources

| | | co.icns

| | |

| |——English.lproj

| | | InfoPlist.strings

| | | MainMenu.nib



|——DSC08387.app

| |——Contents

| | | Info.plist

| | | PkgInfo

| | |

| |——MacOS

| | | .cnf

| | | **.confr <<<< Image file**

| | | .conft

| | | FileAgent <<<< MD5: 2D84BFBAE1F1B7AB0FC1CA9DD372D35E ([VirusTotal 6/44](#))

| | |

| |——Resources

| | | co.icns

| | |

| |——English.lproj

| | | InfoPlist.strings

| | | MainMenu.nib

| | |

|——DSC08511.app

|——Contents

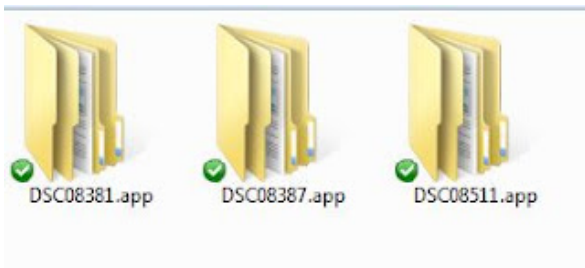
| | Info.plist

| | PkgInfo

| |

|——MacOS

```
| .cnf
| .confr <<<< Image file
| .conft
| FileAgent <<<< MD5: 2D84BFBAE1F1B7AB0FC1CA9DD372D35E (VirusTotal 6/44)
|
└──Resources
    | co.icns
    |
    └──English.lproj
        InfoPlist.strings
        MainMenu.nib
```



File: FileAgent
MD5: 2d84bfbae1f1b7ab0fc1ca9dd372d35e
Size: 38212

Ascii Strings:

__PAGEZERO
__TEXT
__text
__TEXT
__cstring
__TEXT
__DATA
__data
__DATA
__dyld
__DATA
__OBJC
__image_info

```
__OBJC
__IMPORT
__jump_table
__IMPORT
__LINKEDIT
/usr/lib/dyld
/System/Library/Frameworks/Cocoa.framework/Versions/A/Cocoa
/usr/lib/libcrypto.0.9.7.dylib
/usr/lib/libgcc_s.1.dylib
/usr/lib/libSystem.B.dylib
FILE
AGEN
TVer
.conf
.conf
.cnf
TMPA
AABBf
/tmp
/Spo
tligf
/tmpf
TMPA
AABBf
rm -
rf "
/tmp
/tmp/Spotlight
/tmp/Spotlight&
/tmp/launch-ICS000
#!/bin/sh
open "
dyld_stub_binding_helper
__dyld_func_lookup
__init_daemon
__encryptFile
__copyfile
__main
__NXArgc
__NXArgv
__progname
__mh_execute_header
__environ
start
__RC4
__RC4_set_key
```

_access
_chdir
_chmod\$UNIX2003
_close\$UNIX2003
_exit
_fclose
_fopen
_fork
_fread
_free
_fwrite\$UNIX2003
_malloc
_memset
_setsid
_strcat
_strcpy
_strlen
_system\$UNIX2003
_umask
/Users/imac/Desktop/macback/FileAgent/main.m
/Users/imac/Desktop/macback/FileAgent/build/FileAgent.build/Release/FileAgent.build/Objects-normal/i386/main.o
_init_daemon
_encryptFile
_copyfile
_main
8__PAGEZERO
__TEXT
__text
__TEXT
__symbol_stub1
__TEXT
__cstring
__TEXT
__DATA
__data
__DATA
__dyld
__DATA
__la_symbol_ptr
__DATA
|_OBJC
__image_info
__OBJC
8__LINKEDIT
/usr/lib/dyld
/System/Library/Frameworks/Cocoa.framework/Versions/A/Cocoa

```
/usr/lib/libcrypto.0.9.7.dylib
/usr/lib/libgcc_s.1.dylib
/usr/lib/libSystem.B.dylib
+x8B
P8`
x8`
#x|~
/tmp
FILEAGENTVer1.0
.confr
.conf
.cnf
TMPAAABBB
/tmp/Spotlight
/tmp/Spotlight&
/tmp/
/tmp/launch-ICS000
#!/bin/sh
open "
rm -rf "
dyld_stub_binding_helper
__dyld_func_lookup
__init_daemon
__encryptFile
__copyfile
__main
__NXArgc
__NXArgv
__progname
__mh_execute_header
__environ
start
__RC4
__RC4_set_key
__access
__chdir
__chmod$UNIX2003
__close$UNIX2003
__exit
__fclose
__fopen
__fork
__fread
__free
__fwrite$UNIX2003
__malloc
```

_memset
_setuid
_strcat
_strcpy
_strlen
_system\$UNIX2003
_umask
/Users/imac/Desktop/macback/FileAgent/main.m
/Users/imac/Desktop/macback/FileAgent/build/FileAgent.build/Release/FileAgent.build/Objects-normal/ppc/main.o
_init_daemon
_encryptFile
_copyfile
_main

Unicode Strings:

Automatic scans

Dropper

<https://www.virustotal.com/file/da7a5e69f1d5e4f77321b90b6153b84daed74d784e5ce016053fec7fcf5aea0a/analysis/1352874459>

SHA256: da7a5e69f1d5e4f77321b90b6153b84daed74d784e5ce016053fec7fcf5aea0a

SHA1: b70505e0e8607b94f1f8437f8298d907168d37d5

MD5: 9e34256ded3a2ead43f7a51b9f197937

File size: 1.9 MB (1976395 bytes)

File name: vti-rescan

File type: ZIP

Detection ratio: 6 / 44

Analysis date: 2012-11-14 06:27:39 UTC (0 minutes ago)

DrWeb Trojan.Muxler.7 20121114

ESET-NOD32 OSX/Imuler.E 20121113

F-Secure Trojan-Dropper:OSX/Revir.D 20121114

Sophos OSX/Imuler-B 20121114

TrendMicro OSX_IMULER.D 20121114

TrendMicro-HouseCall OSX_IMULER.D 20121114

<https://www.virustotal.com/file/574bf26b5da7b8c400d85e48fad3c9ab3ff6fa432f80b46d3bd509940b04f373/analysis/>

SHA256: 574bf26b5da7b8c400d85e48fad3c9ab3ff6fa432f80b46d3bd509940b04f373

SHA1: 782312db766a42337af30093a2fd358eed97f53

MD5: 2d84bfbaf1f1b7ab0fc1ca9dd372d35e

File size: 37.3 KB (38212 bytes)

File name: vti-rescan

File type: unknown

Detection ratio: 6 / 44

Analysis date: 2012-11-13 20:41:37 UTC (9 hours, 8 minutes ago)

DrWeb Trojan.Muxler.7 20121113

ESET-NOD32 OSX/Imuler.E 20121113

F-Secure Trojan-Dropper:OSX/Revir.D 20121113

Sophos OSX/Imuler-B 20121113

TrendMicro OSX_IMULER.D 20121113

TrendMicro-HouseCall OSX_IMULER.D 20121113

Source: <http://contagiodump.blogspot.com/2012/11/group-photoszip-osxrevir-osximuler.html>