OSX/Imuler updated: still a threat on Mac OS X

welivesecurity.com/2012/03/16/osximuler-updated-still-a-threat-on-mac-os-x/

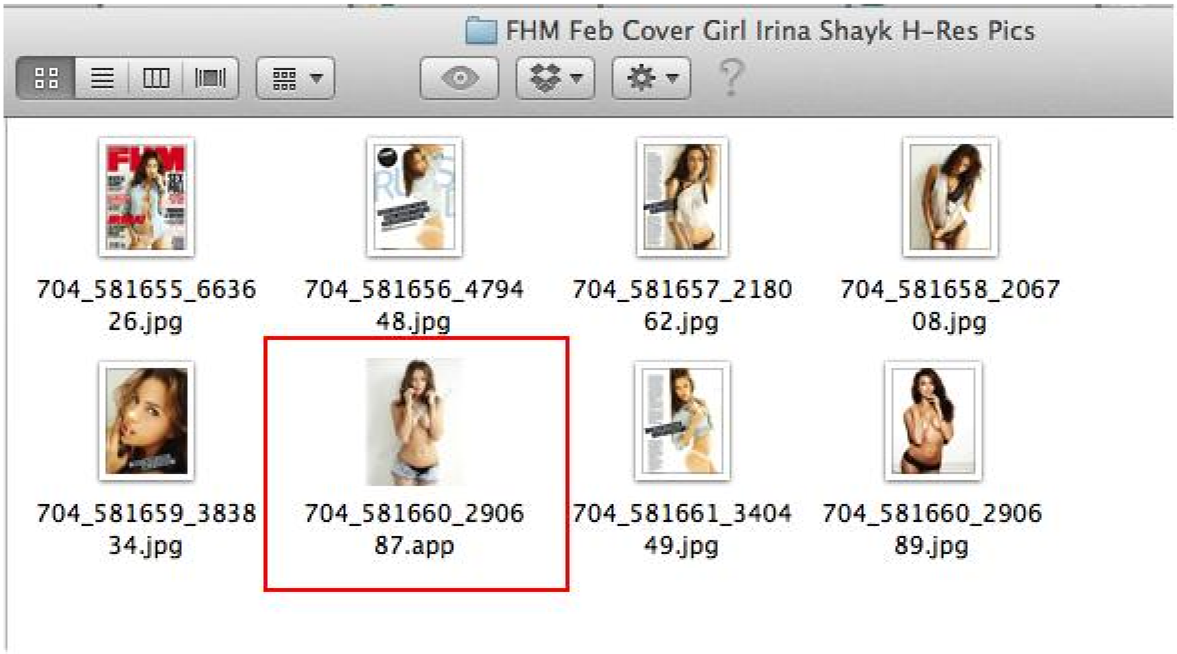
March 16, 2012

A new variant of Mac information-stealer OSX/Imuler hides itself inside a ZIP archive, right in the middle of an array of erotic pictures.

16 Mar 2012 - 10:02AM

A new variant of Mac information-stealer OSX/Imuler hides itself inside a ZIP archive, right in the middle of an array of erotic pictures.

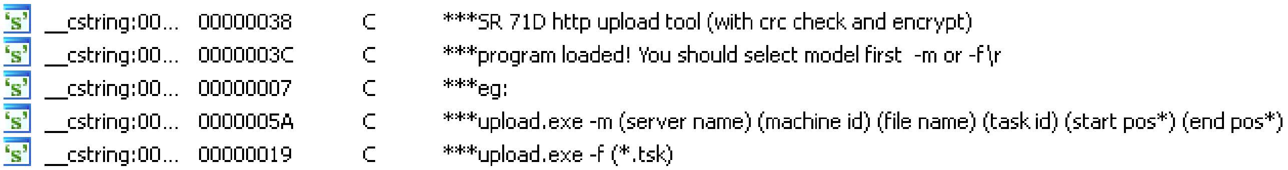
The Mac OS X information stealing malware OSX/Imuler, initially discovered last fall, has resurfaced. This time, instead of being installed by the OSX/Revir.A dropper, this new variant of OSX/Imuler hides itself inside a ZIP archive, right in the middle of an array of erotic pictures, waiting for the user to open the malicious application.



This new variant is very similar to its ancestors in terms of command-and-control (C&C) communication and functionalities. (OSX/Imuler is an information stealer that can gather and transmit files, screenshots, and other data to a remote server.) The network protocol is still HTTP-based and the payload is compressed with zlib. The hardcoded C&C domain now being used is a new one, registered on February 13th, 2012 via a Chinese registrar. The domain points to the same IP address as the previous variants, located in the USA and still active at time of writing.

This all seems to indicate that the new variant was most likely released to improve its anti-virus evasion.

OSX/Imuler has the functionality to upload arbitrary local files to the C&C. A specialized separate executable named CurlUpload, downloaded from the C&C every time the malware starts, is used to perform the operation. This stand-alone executable, first seen in early 2011, presents interesting strings that suggest it was initially built for Win32 but later recompiled for OS X:



```
__cstring:00...  00000038   C   ***SR 71D http upload tool (with crc check and encrypt)
__cstring:00...  0000003C   C   ***program loaded! You should select model first  -m or -f\r
__cstring:00...  00000007   C   ***eg:
__cstring:00...  0000005A   C   ***upload.exe -m (server name) (machine id) (file name) (task id) (start pos*) (end pos*)
__cstring:00...  00000019   C   ***upload.exe -f (*.tsk)
```

ESET security software (including ESET Cybersecurity for Mac) since signature update 6970 detects this new variant as OSX/Imuler.C.

MD5 of the files analyzed:

7dba3a178662e7ff904d12f260f0fff3 (Installer)
9d2462920fdaed5e360875fb0cf8274f (malicious payload))
e00a280ad29440dcaab42ad093bcaafd (uploader module)

Big thanks to my colleague **Marc-Étienne M. Léveillé** for his work on this investigation.

Alexis Dorais-Joncas

16 Mar 2012 - 10:02AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion