a cura di: **Salvatore Campolo - Totocellux - 27-02-2012 11:55**

Il Trojan horse MAC Flashback è tornato ad infettare Apple Mac OS X

LINK (https://www.nexthardware.com/news/antivirus/4394/il-trojan-horse-mac-flashback-e-tornato-ad-infettare-apple-mac-os-x.htm)

Intego, azienda focalizzata sulla sicurezza in ambienti Apple, avverte sul ritorno del malware MAC Flashback (OSX/Flashback.G).

L'azienda americana Intego (http://www.intego.com/), specializzata nell'ambito della sicurezza dei sistemi operativi Apple sin dal 1997 e creatrice dei prodotti Virus Barrier (http://www.intego.com/virusbarrier/) ed Internet Security Barrier (http://www.intego.com/internet-security-barrier/), ha inserito un post sul proprio blog in data 24 febbraio 2012, dopo aver avuto, proprio tramite questi software, svariati riscontri positivi di una nuova infezione.

Tramite appunto le pagine del proprio blog, Intego ha voluto mettere in guardia gli utilizzatori di prodotti MAC ed in generale di sistemi operativi dell'azienda di Cupertino, sulla nuova apparizione dell'ormai famoso trojan horse MAC Flashback, affacciatosi alle porte della Mela sin dal settembre del 2011 con il capostipite OSX/Flashback.A.

↔

↔

Il malware, giunto alla variante OSX/Flashback.G, riesce attualmente ad utilizzare ben tre distinti metodi di infezione, sfruttando eventualmente delle falle presenti sulla macchina da infettare ed utilizzandole a seconda del livello di sicurezza dei sistemi operativi MAC OS X 10.x.

In particolare, OSX/Flashback.G sfrutta in prima analisi, ove presente, una vulnerabilità nell'implementazione della versione Java installata su Snow Leopard e, dove non fosse possibile utilizzarla, appare abilmente congegnato per camuffarsi da installazione di un certificato digitale.

Tale certificato viene direttamente visualizzato presentando le credenziali di Apple Inc. e, sfruttando le oramai note strategie di ingegneria sociale sull'eventuale sprovveduto utente di turno, il trojan horse è così riuscito in molti casi a farsi installare.

A quel punto il malware riesce facilmente a modificare il browser e le applicazioni di rete al fine di trafugare ed inviare all'esterno tutte le possibili credenziali di accesso utilizzate dall'utente: tra queste è stato possibile stabilire che le prime ad esser ricercate dal malware siano quelle di Google, Yahoo!, CNN, PayPal ed altre ancora.

In soccorso di tutti gli utilizzatori di personal computer e sistemi operativi della Mela, questo (http://blog.intego.com/flashback-mac-trojan-horse-infections-increasing-with-new-variant/) è il link al blog di Intego dove è possibile approfondire la questione, nonché trovare i possibili rimedi da metter in atto in base all'infezione attuale, mentre qui (http://blog.intego.com/intego-security-memo-%E2%80%93-september-26-2011-mac-flashback-trojan-horse-masquerades-as-flash-player-installer-package/) è possibile informarsi sulle caratteristiche dell'infezione di OSX/Flashback.A, risalente al settembre 2011.↔

↔

↔