

WebSense 安全實驗室：不肖駭客利用米高積遜死訊，

散發垃圾郵件與木馬程式！

人「死」是非多?! 流行音樂天王米高積遜驟逝的消息震撼全球，間接造成所有相關音樂影片、新聞網頁攻佔網路熱門點擊、搜尋排行榜。不肖駭客當然也沒有放過這樣的機會，以「從未公開的米高積遜影片、圖片」為餌，大發惡意郵件，藉機以木馬病毒攻佔使用者電腦。WebSense 呼籲，使用者切莫因為一時熱潮就點擊、下載不明連結，讓自己的電腦成為米高積遜之死的受害對象！

WebSense Security Labs(TM) ThreatSeeker(TM) Network 發現，近來有垃圾郵件謊稱內含「從未公開的米高積遜影片、圖片」，並提供偽造的 YouTube 連結，誘使使用者下載木馬程式。

WebSense 表示，這個木馬程式名為 *Michael.Jackson.videos.scr* (MD5:664cb28ef710e35dc5b7539eb633abca)，被放置於一個澳洲的合法廣播網站之中，使用者執行該檔案後，預設瀏覽器會彈出與米高積遜死訊有關的合法新聞網頁 (<http://musica.uol.com.br/ultnot/2009/06/25/michael-jackson.jhtm>)，讓使用者卸下警覺。事實上，在使用者開啓該網頁的同時，會有 3 個盜竊使用者個人資料的惡意元件，悄悄地在底層執行並安裝。

這些木馬程式之中，包含一個防毒警覺率非常低的 michael.gif 檔案(相關病毒資料詳見：[這裡](#))，這會導致使用者安裝一個惡意的 BHO，會與 %windir%/Dynamic.dll 註冊在一起，並產生識別項(GUID)名稱{FCADDC14-BD46-408A-9842-CDBE1C6D37EB}。至於另外兩個元件，一個會在開始功能表中執行 %windir%\system32\kproces.exe，另一個則會經由惡意程式安裝 %windir%\system32\fotos.exe 惡意檔案。

所有 WebSense® Messaging 與 WebSense Web Security 的客戶，都已受到完善的防護，亦不會受到此波攻擊的影響。然而，WebSense 仍要呼籲，尚未擁有 WebSense 安全防護的用戶，最近對於相關的米高積遜影片、圖片、新聞連結，都應該要多加警覺。如欲閱讀更詳細的相關資料，歡迎前往 [WebSense Security Labs](#) 瀏覽。



Websense 公司簡介

Websense, Inc. (那斯達克：WBSN) 是網頁過濾、資料保護及郵件安全解決方案的領導廠商，為全球超過 4,400 萬的企業員工，提供 Essential Information Protection™ 解決方案。透過全球各地的合作夥伴，Websense 安全解決方案軟體主動幫助企業阻止惡意代碼，預防機密資料遺失和執行網路使用的安全政策。如欲獲取更多資料，請瀏覽 www.websense.com。