張元成

寄件者: 國家資通安全會報技術服務中心 <ncert@icst.org.tw>
寄件日期: 2013年8月6日星期二 下午 5:42
收件者: ncert@icst.org.tw
主旨: [資安訊息警訊] 國家資通安全會報技術服務中心（事件編號：ICST-ANA-2013-0018)
簽名者: ncert@icst.org.tw

國家資通安全會報 技術服務中心

漏洞/資安訊息警訊

發布編號	ICST-ANA-2013-0018	發布時間	Tue Aug 06 17:16:06 CST 2013
事件類型	攻擊活動預警	發現時間	Tue Aug 06 00:00:00 CST 2013
警訊名稱	播放軟體 KMPlayer 更新機制異常，請各單位注意並提高警覺		
內容說明	技服中心接獲外部情資，播放軟體 KMPlayer 更新機制異常，駭客疑似透過播放軟體 KMPlayer 更新機制散播惡意程式。 KMPlayer 執行後，若出現版本 3.7.0.87 更新訊息，將連線至 http://cdn.kmplayer.com/player/update 下載偽冒更新程式(KMP_3.7.0.87.exe)。 偽冒更新程式執行後，並不會變更原 KMPlayer 版本，但將植入惡意程式於下述資料夾(預設隱藏)： Windows XP C:\Documents and Settings\All Users\OleView\ACLUI.DLL C:\Documents and Settings\All Users\OleView\ACLUI.DLL.UI C:\Documents and Settings\All Users\OleView\OleView.exe Windows 7 C:\ProgramData\OleView\ACLUI.DLL C:\ProgramData\OleView\ACLUI.DLL.UI C:\ProgramData\OleView\OleView.exe 目前已知受感染電腦會連線以下中繼站: -pen.abacocafe.com		

	-pens.abacocafe.com -cdn.abacocafe.com -vpen.abacocafe.com KMPlayer 源自韓國的一套播放軟體，最新版本為 3.6.0.87，支援各種常見的影音檔播放，且內建多國語系，由於使用情況相當普遍，影響範圍與衝擊不容小覷。請各機關立即清查機關內是否有連線上述中繼站的行為，若發現中繼站連線或異常行為，請立即至通報應變網站（https://www.ncert.nat.gov.tw）進行資安事故通報。
影響平台	所有 KMPlayer
影響等級	高
建議措施	1.若發現上述惡意程式，請盡速刪除，或可透過下述防毒軟體進行偵測： (1)OfficeScan(趨勢科技) 病毒碼版次：CPR 10.200.01 (2)SmartScan(趨勢科技) 病毒碼版次：TBL 13436.002.00 (3)Avira 病毒碼版次：7.11.94.64 2.更新播放軟體 KMPlayer 時，注意更新版次是否與官網相符(目前官方最新版本為 3.6.0.87)。 3.此攻擊事故已通知韓國相關單位，目前尚未接獲進一步處理說明，建議暫時停用多媒體播放軟體 KMPlayer，改用其他播放軟體。
參考資料	無

此類通告發送對象為通報應變網站登記之資安聯絡人。若貴 單位之資安聯絡人有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安聯絡人但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)
地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@icst.org.tw