微軟 Windows 作業系統零時差弱點 CVE-2014-4114

(一) 預警說明：

據調查顯示，一個俄羅斯的駭客團體已透過此一漏洞來發動攻擊活動(Sandworm) ，目標是竊取與攻擊北大西洋公約組織(NATO)與歐盟等企業與重要人士的資料。 這項漏洞存在於 Windows 作業系統中的 OLE Package Manager，透過 Office PowerPoint 文件觸發該漏洞，會下載並執行特定的 INF 檔案，並下載任意程式碼。

(二) 影響等級：

高

(三) 影響平台：

此漏洞影響 Vista 之後所有版本的 Windows 作業系統 與 Windows Server 2008 及 2012。

(四) 建議措施：

趨勢科技產品已經可以偵測利用此漏洞的病毒程式，病毒名稱為”TROJ_MDLOAD.PGTY” 。當開啟駭客製作的 Power Point 檔案之後，會下載一個 INF 檔惡意程式(被偵測為” INF_BLACKEN.A”)，並嘗試下載與執行一支被偵測為”BKDR_BLACKEN.A”的後門程式。 詳細病毒資訊請參考下列連結。

TROJ_MDLOAD.PGTY

http://about-threats.trendmicro.com/malware.aspx?language=en&name=TROJ_MDLOAD.PGTY

INF_BLACKEN.A

http://about-threats.trendmicro.com/malware.aspx?language=en&name=INF_BLACKEN.A

BKDR_BLACKEN.A

http://about-threats.trendmicro.com/malware.aspx?language=en&name=BKDR_BLACKEN.A

由於此一攻擊方式並不特別複雜，很有可能導致駭客們大量濫用，建議用戶盡快針對此一 Windows 作業系統的漏洞進行修補，在完成修補前，不要隨意開啟陌生人寄來的 PowerPoint 檔案，以降低被攻擊的風險。