

Sept 2005

阻擋Zotob，找Cell Technology就對了

ZOTOB系列病毒是有始以來在微軟漏洞公佈後最快散播的病毒，目前已經在全球傳染開來，在台灣也有不少感染案例。當病毒執行時，利用了Windows UPnP 當中的漏洞，會自動放置一份病毒副本到Windows System目錄下，檔名為WINTBPEXE，此病毒還會建立登錄檔機碼，以在系統啟動時載入這個檔案，使得病毒作者可從遠端遙控執行，而且電腦螢幕上並不會因此產生任何異樣，一般使用者無法從電腦上即時判斷是否已經遭受到病毒感染。除此之外，ZOTOB.C還會在電腦中蒐尋含有David、James等電子郵件信箱來進行散播。

Cell Technology研發團隊在第一時間研究病毒散播特性，製作特徵碼並提供線上下載，將IPS架設在Internet進出口，可以有效協助您建立第一道偵測與阻擋該病毒的防線，也可部署在企業內部，有效防堵該病毒的擴散。

不只是偵測與阻擋，更要修補漏洞，Cell SPM是協助你建立補充程式管理機制的最佳選擇，藉由主動的掃描方式，全面清查企業內部未上該補充程式的電腦，你可快速有效掌握企業風險並在第一時間強制安裝所需的補充程式。

<http://www.cell-technology.net/>

Sept 2005

Cell Technology宣佈ArcSight為資安事件管理方案合作夥伴

ArcSight (www.arcsight.com) 是資安事件管理系統的廠商，可將完整的資安事件匯集、修正、意外事件回應和回報功能都整合在單一解決方案中。客戶可以使用ESM產品收集多個資安設備 (比如說防火牆、入侵偵測與防禦系統等等)

的事件進行相關聯性分析，包括資產價值與弱點狀態，具備自動的調查資安事件與提供解決方案能力，並產生專業報表。

Cell Technology很榮幸的宣布自今年七月開始，ArcSight ESM支援Cell IDS與IPS全系列產

品，整合Cell IDS與IPS所偵測到的事件在單一主控台中，進行完整的事件分析與報表展示，有助於Cell Technology與ArcSight雙方在電信與大型企業資訊安全專案的進一步合作

<http://www.cell-technology.net/>