



<http://news.networkmagazine.com.tw/classification/security/2011/11/18/35737>

面對APT威脅 Palo Alto推出「野火」雲端惡意軟體分析服務

謝至恩

/ 普吉島報導

- 2011/11/18分類：[安全防護](#), [新聞](#), [頭條](#)

當今安全產業界面臨的最大敵人，莫過於「先進持續攻擊 (Advanced Persistent Threat)」所造成的危害。由於APT攻擊多半屬於客製化攻擊，因此具備隱藏性高、演化快速的特質，因此企業往往無從察覺正在遭受到APT攻擊，直到損害發生。

Palo Alto Networks創辦人暨技術長Nir

Zuk在NetEvents亞洲會議上表示：「目前的安全管理服務已經能夠有效管理病毒大規模爆發的情況，甚至能夠提供服務水準協議(Service Level Agreement, SLA)，但對於當今流行的APT攻擊則束手無策，最主要的原因是一般的IPS與過濾掃描方案，無法有效辨識出所有的應用流量，以及偵測未知惡意軟體的能力不足。」

Nir Zuk解釋，為了能夠有效偵測出未知的惡意軟體，Palo Alto

Networks決定將實驗室中的沙箱技術，放到現實環境，推出名為「野火(WildFire)」的雲端惡意軟體分析引擎，透過上千顆處理器的運算能力，

在雲端建立**虛擬環境 - 也就是沙箱(sandbox)**，將Palo Alto

Networks次世代防火牆自動搜集到的可疑文件與程式，放入沙箱中執行，並分析其磁碟行為與網路流量行為。若發現到惡意行為，足以判斷該可疑軟體為惡

意軟體，便立即自動為該惡意軟體與其網路流量行為**產生特徵碼**，立即佈署到所有客戶的Palo Alto Networks次世代防火牆上。