



中信國際電訊CPC及合作伙伴合辦網絡保安論壇

了解業界前沿趨勢

智選應對

APT解決方案



Executive Panel Discussion

Unravel the myth of APT:
The best way to combat APT attack



■(左起) 中信國際電訊CPC信息科技及安全服務部高級副總裁鄭偉基、Palo Alto Networks香港及澳門區總經理王衍恒、Imperva亞太及日本區安全系統總監Vladimir Yordanov及中信國際電訊CPC銷售部高級副總裁鄧志明就如何應對APT作出了深入探討。

由 中信國際電訊CPC、Imperva與Palo Alto Networks聯合舉辦，旨在探討預防及應對進階持續性滲透攻擊（APT）的網絡保安論壇已經於十一月十四日圓滿舉行。是次會議除邀得三間信息安全產品及服務供應商的代表分析業界最新趨勢外，也邀請了會計界及法律界專家，從企業的角度分享預防APT的重要性。整個會議氣氛熱烈，專家的發言及回答提問環節除觸及多個網絡保安的核心議題，也深入淺出地介紹了各種最新的預防APT方案。

APT網絡攻擊日益猖獗 企業防範意識不足

APT攻擊的其中一個特性是隱蔽性高，企業因一般難以察覺當中的安全威脅，往往疏於防範。然而，即使APT攻擊受到較少注意，它對網絡信息安全及企業利益卻有很大威脅，例如最近業界經常討論的「DarkHotel」個案，便反映了APT攻擊日漸成熟且無處不在的危險性。中信國際電訊CPC銷售部高級副總裁鄧志明在致辭時也指出，不論是亞洲的「DarkHotel」個案，抑或更早前荷李活明星遭竊取個人生活照的事件，都反映APT攻擊日益嚴重。論壇主持、羅兵咸永道會計師事務所合夥人黃景深也引述羅兵咸永道的研究報告，指出本港近半企業並未有預防APT的方案，情況讓人憂慮。

APT轉趨專業化 雲端系統勢成戰場

三位主講嘉賓都認同現時企業的防範仍然不足，難以應付日新月異的APT攻擊。中信國際電訊CPC信息科技及安全服務部高級副總裁鄭偉基指，現時企業的一大問題是缺乏對APT的了解，例如不少公司誤以為僅靠防毒軟件及一般防火牆便足以防禦APT。Imperva亞太及日本區安全系統總監Vladimir Yordanov也對此表示認同。他再次引用「DarkHotel」的個案，指出APT的攻擊於近年已大為成熟，由過往沒有特定目標，甚至純粹戲弄的性質，轉變成為有特定目標、精密組織的商業性犯罪性質主導。他指：「作為信息安全產品的供應商，當務之急是做好偵測及防範（Detection and Prevention）的解決方案，並同時提升大眾對網絡保安議題的認識。」

Palo Alto Networks香港及澳門區總經理王衍恒也認同APT攻

擊的情況於近年有很大變化，企業不容忽視。他指：「以往的APT攻擊的玩樂性質較重，但現時則多為商業利益，又或就某些政治議題進行攻擊。再者，網絡上有大量APT攻擊的教學，甚至有不少APT的代理組織，因此無論任何一間企業也不能置身事外。」他也指出隨著流動裝置的普及，未來會有愈來愈多針對雲端系統及流動操作系統的攻擊，威脅企業的信息安全。

外判網絡保安公司 宜審慎挑選

不少企業由於對網絡保安的認知不足，因此會選擇將網絡保安事宜外判，以節省成本。然而，不少企業往往忽視了自己的責任，帶來不少潛在風險。王衍恒指出，對不少缺乏IT專才的企業而言，外判是可行做法。不過企業必須知道哪些資訊內容是可以安全外判的，避免機密資料外泄。Vladimir Yordanov及與會的品誠梅森律師事務所合夥人Paul Haswell也不約而同地指出，外判保安工序並不能「外判法律責任」，其中Paul Haswell更引用新加坡的案例，說明即使是由第三方把資料外泄，相關企業仍難逃法律責任。鄭偉基補充時指，不少企業會自行聘請IT人員，建構自己的保安系統。然而，這方法成本高昂，而且企業保安程度難以與專業媲美。因此，較可取的做法，是慎選方案供應商，並瞭解公司的機密資料所在。

Assurance-as-a-Service 對抗APT之選

一個完善的信息安全解決方案，應該具備三項特質：預防偵測、修正及簡易操作。其中Imperva與Palo Alto Networks的方案集中在APT的預防及偵測上，而中信國際電訊CPC則透過其安全管理

服務，提供先進的安全信息與事件管理（SIEM）技術，以及簡易使用的用戶儀表板，為企業提供精準、易操作的信息安全解決方案。鄭偉基在研討會中提出「Assurance-as-a-Service」的概念，意即透過結合先進的APT預防及偵測技術、安全管理服務，並加上獲得安全認證的專家團隊，配以信息評估服務為客戶作漏洞管理，便可為客戶帶來「Assurance-as-a-Service」（「信心即服務」），令客戶可輕鬆應對各種網絡攻擊及挑戰。



■是次會議觸及多個信息安全的重要議題，包括針對雲端系統的APT防禦，以及關於APT的真實個案分析。