資安威脅升級至國家等級

比駭客更駭人的惡意程式

文／施鑫澤

現代網路戰爭逐漸萌芽，企業所需具備的資安防護應再強化，以避免遭受魚池之殃。

場北韓網路攻擊南韓的事件，把原本已經風聲鶴唳的資安議題再度延燒，現代戰爭更已經把網路攻擊當作重要的試探性手段，對經濟主幹進行攻擊，這就類似此次的南韓電視台等重要企業一般，加上難以舉證，因此相信在不久的將來，「網軍」必將一一浮現在世人面前，身為企業的重要資安防護決策者，如何在此趨勢發展下，佈署固若金湯的防護機制，正困擾著資訊長、安全長們。

從2013年CIO IT決策者關鍵報告中，不管是雲端或BYOD，安全均為最重要的考量，北韓此次網攻事件雖然雷聲大雨滴小，但是整整四月，從月初開始，資安廠商便陸續發聲，發表各項資安報告，提醒企業不可不慎，當然同時也介紹自家公司的應對方案。其中，尤其外商資安業者過去或許鴨子滑水，僅在幾個大企業間溜轉，看好此一商機，也都一一現身，後面將逐一介紹，以供參考。

資安報告 震撼教育

資安廠商的報告由來已久，面對逐漸升溫的資安威脅，此時的報告便相形重要，列舉數家趁此機會發表自家的報告內容做參考。

Blue Coat
2013年行動惡意軟體報告

以網安及廣域網路優化方案見長的Blue Coat於月初發表2013年行動惡意軟體報告，報告中顯示，高達三分之二的行動攻擊源於惡意網路，提醒企業安全防護範圍應擴及行動設備並加強存取權限控管。報告內容包括以下主題：

- 行動設備和行動應用的特性，使它們更容易受到多種特定類型攻擊的侵害。
- 最成功的行動惡意軟體手段包括詐騙、垃圾郵件和網路釣魚。
- 這些曾經出現在Web上的典型攻擊活動，不受設備所限且易於部署，讓網路犯罪分子能針對行動設備發動攻擊。
- 使用者可以透過傳統網頁、行動版網頁、本端應用程式等多種方法造訪相同內容，這使得行動設備的保護與管理更加複雜。
- 色情內容是行動使用者的最致命弱點。當使用者造訪色情網站時，他們遭受攻擊的風險會比其他行為高出近三倍。
- 網路犯罪分子開始將目光投向行動用戶。2012 年時，有將近三分之二的行動攻擊源於惡意網路，其中 40%是已知的惡意網路。

這資料來自 Blue Coat WebPulse協作防禦和 Blue Coat的安全實驗室。WebPulse 對來自全球 7,500萬名用戶的查詢要求進行了即時分析，進而全面瞭解網路和惡意軟體生態系統。

Akamai
2012年第四季報告

以雲端優化服務主的Alamai，則發表去年第四季的觀察報告，報告中顯示，分散式阻斷服務（DDoS）攻擊年增長超過兩倍，

Akamai提醒，現今由原IP位址識別的攻擊來源可能並不能代表攻擊者所真正居住的國家。例如，一個在美國的人可能發起來自中國被入侵系統的攻擊。

2012年第四季，Akamai觀察發現來自177個國家/地區的攻擊流量，較第三季的有所減少。中國仍然是Akamai觀察到的最大攻擊流量來源，佔總數的41%，比上一季的33%有所增加。美國仍排在第二，其觀察到的攻擊流量從第四季佔13%降至10%。俄羅斯取代土耳其居第三的位置，其攻擊流量佔4.7%。

本季排名前10的不同國家地區所產生的攻擊流量佔觀測到的總攻擊流量的75%，中國和美國佔據略超過50%的總攻擊流量。

該季Port 445（微軟-DS）遭受29%的攻擊流量，仍是最容易遭受攻擊的目標埠。Port 23（Telnet）名列第二，佔7.2%。

去年(2012年)，Akamai客戶報告了768次DDoS攻擊，比2011年增加了兩倍。其中，35%的目標公司在商貿業，22%則是媒體及娛樂公司。包括金融服務業在內的企業占20%，高科技公司占14%，9%則直接指向公家機構。

賽門鐵克
全球網路安全威脅研究報告

賽門鐵克發表全球網路安全威脅研究報告(Internet Security Threat Report, ISTR)，報告指出2012年針對式攻擊數量激增，較前一年成長42%，這些針對性的網路間諜攻擊大多鎖定中小企業，並藉由「水坑攻擊」手法，最終達到竊取大型企業智慧財產權的目的。

報告顯示，2012年針對250位員工以下的中小企業發動的攻擊次數佔總攻擊數量的三成，較2011年增加13%，而針對式攻擊最常鎖定的產業是製造業，佔所有針對性攻擊的24%，較前一年增加六成。此外，針對行動裝置的惡意程式數量更是激增58%。

台灣賽門鐵克資深技術顧問張士龍表示，在台灣方面，台灣整體網路威脅名列全球第九名，台灣殭屍網路的數量則是全球第三，是台灣網路安全的一大隱憂。

他指出，多項發現顯示網路犯罪狀況並沒有減緩，反而竊取資料的手法愈加精密複雜，加上虛擬化、行動應用、雲端運算趨勢使得企業IT環境日益複雜，讓企業必須積極面對安全防護，並主動提升防護層級，方可預防可能發生的攻擊事件。

Fortinet 威脅季報

以提供高效能網路安全的Fortinet，根據其FortiGuard Labs公佈的威脅季報顯示，由全球FortiGate網安設備所回報的情資中呈現，虛擬貨幣Bitcoin挖礦殭屍網路ZeroAccess為今年第一季主要的網路威脅。雖然，台灣對於虛擬貨幣Bitcoin並不熱衷，但是仍要小心企業伺服器成為DDoS感染的主機，成為功擊的幫兇與跳板。

對於南韓企業被網攻事件，Fortinet季報指出，由於大量的惡意軟體攻擊南韓電視台和金融機構，造成大規模的損害，抹除了上千個硬碟資料。

FortiGuard Labs透過與南韓公、私部門的關係，已揭露其攻擊特性與惡意軟體如何擴散的相關資訊。其研究結果顯示，攻擊者能取得更新管理系統的控制權，並藉著這些受信任的系統，散佈惡意軟體至鎖定攻擊的目標網路。

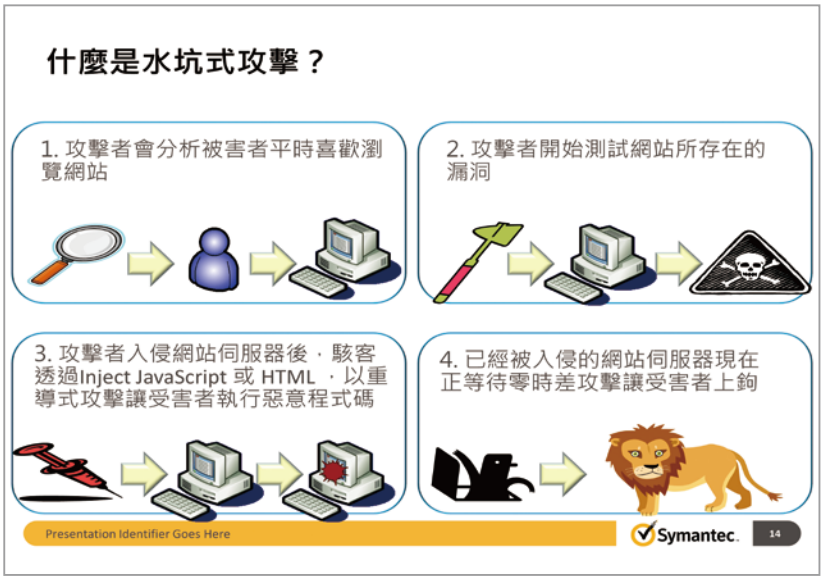
FortiGuard Labs資深防毒經理Kyle Yang表示，在調查這些攻擊時，我們發現有一種版本的wiper惡意軟體能染感內部的安全管理伺服器，並利用其受信任的特性，在受害者的網路裡肆意散佈。

Fortinet台灣區總經理陳鴻翔形容說，APT攻擊就如同外科手術般細膩並講求精準度，且台灣由於位在網路戰略極為重要的樞紐，相當容易成為攻擊其他國家的跳板。

駭客手段 防不勝防

南韓電視台與金融機構逾三月遭受APT攻擊，約有近五萬台電腦與自動提款機出現故障現象，此一大規模網路攻擊事件，讓APT（Advanced Persistent Threat；進階持續性滲透攻擊）此網路攻擊方式，成為矚目焦點。

對此，趨勢科技與Fortinet便分別提出看法，甫露面的FireEye則提醒新的攻擊態勢，提醒企業與台灣公家機關注意。



資料來源: 賽門鐵克

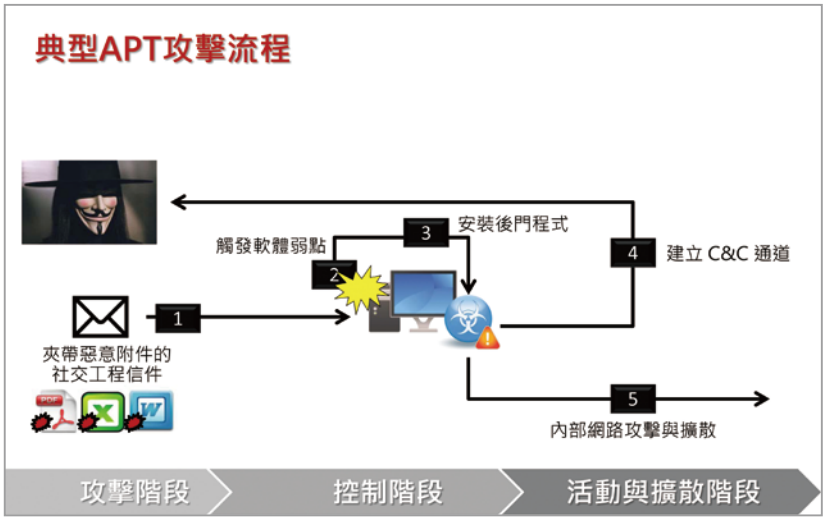
趨勢科技
《客製化防禦策略》

因應APT及針對性攻擊，傳統資安大廠趨勢科技宣布新年度的《客製化防禦策略》（Custom Defense Strategy，CDS)將提供創新的技術，專門偵測並攔截進階持續性滲透攻擊（APT）與鎖定目標攻擊的幕後操縱通訊（C&C)。該公司表示，《客製化防禦策略》(CDS)能夠防範進階威脅的解決方案，不僅讓企業偵測及分析針對性目標攻擊，還能迅速調整其安全防護來回應駭客的攻擊。

趨勢科技台灣暨香港區總經理洪偉淦表示，APT是駭客與防禦端兩造之間，永遠無法停息的戰爭。近期APT大規模網路針對性攻擊事件頻傳，從媒體到資安廠商無一倖免，APT攻擊絕對是企業須立即正視的問題！洪偉淦進一步說明，這場沒有終點的戰爭，企業唯有竭盡所能提高駭客入侵門檻，增強自身防禦能力，以減少駭客入侵的機會。

他指出，靠傳統防禦架構或是單一產品，都不是有效阻擋APT的方法，因此，趨勢科技提出對APT攻擊最新的戰術《客製化防禦策略》(CDS)，針對企業客戶量身打造，率先改善了幕後操縱通訊的偵測與情報能力，並且將這些能力整合到每一項產品當中，提供客戶在對抗駭客時所需的全盤掌控。

趨勢科技推出這套《客製化防禦策略》(CDS)，其中的幕後操縱通訊防範技術，能讓網路、閘道、伺服器及端點等防護點擁有獨特的客製化偵測及防護能力，並且提供集中式警示與幕後操縱風險情報，能隨時掌握及掌控駭客的幕後操縱活動。這是企業第一次擁有偵測及掌握這類重大攻擊的能力，在傷害造成之前預先採取行動。



資料來源: 趨勢科技

只是，由於是客製化，當面對同一時間許多企業被攻擊時，仍會有人力與資源不足的情況，因此，憂心的人可以趕緊去了解與部署此一方案。

Splunk
助南韓企業戰駭客

為了讓台灣企業的資安人員可以獲得第一手、最貼近實戰的資訊，代理Splunk的精誠資訊則於日前舉辦《Splunk 資安事件調查X檔案》研討會，並特別遠從南韓邀請到資安專家 Young Cho (Director of Technical Consulting. MOS in Korea)來台，分享他這次協助南韓企業抵禦駭客攻擊的實戰經驗，如何利用Splunk迅速分析駭客的攻擊軌跡，將企業的風險與損失降至最低。

毋恃敵之不來
恃吾有以待之

網路安全與資安防護進入另一個階段，企業已經不再能像過去買個方案便能解決，重要地反而是內部的資安意識，從趨勢科技對於APT的剖析可看出，最初的漏洞往往是員工的好奇心所致，如何從人員訓練與廠商方案雙管齊下，在在考驗資安人員的智慧，也是需要全面檢討的時機。所幸由於南韓事件，讓我們有了提前警示的效果，後知後覺總比不知不覺好些，期待透過企業自身的努力與資安業者的輔助，讓此不願發生的事件發生時，損傷能降至最低。